IDC MarketScape

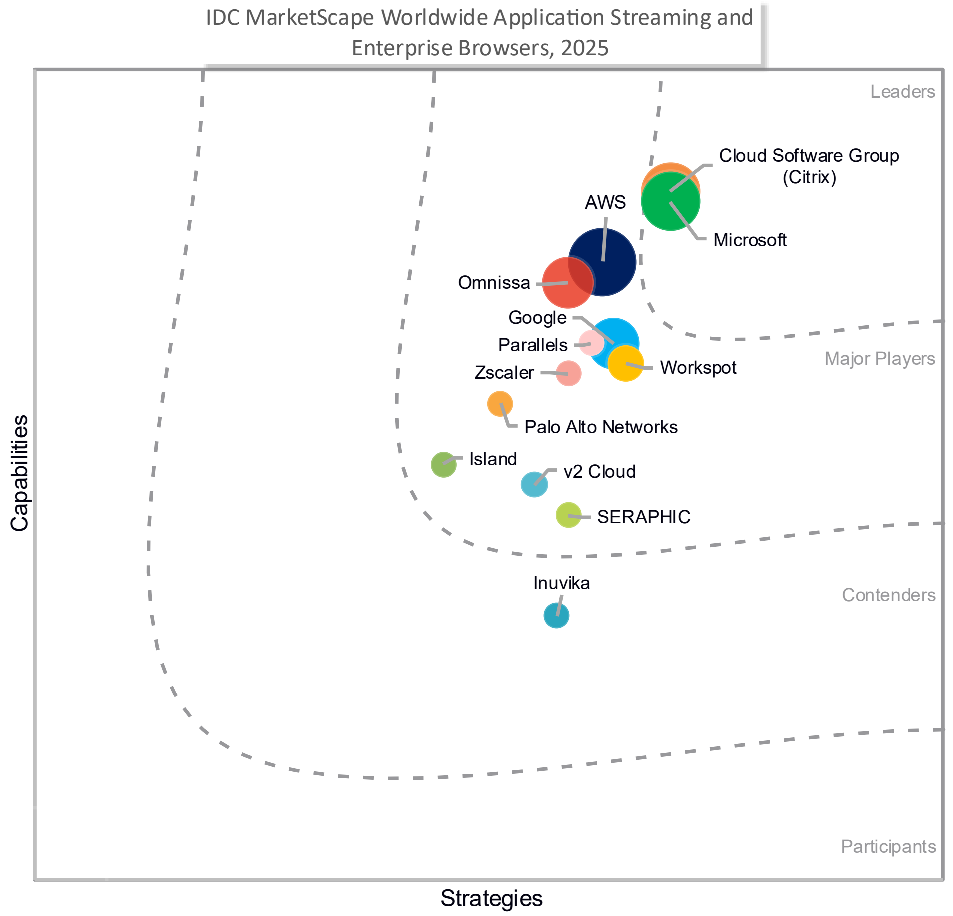
IDC MarketScape: Worldwide Application Streaming and Enterprise Browsers 2025 Vendor Assessment

Shannon Kalvar

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Application Streaming and Enterprise Browsers Vendor Assessment



Source: IDC, 2025

July 2025, IDC #US53004525

See the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

Application streaming and enterprise browsers are two related segments of the rapidly evolving enterprise client computing (ECC) ecosystem. This ecosystem, once mostly encapsulated in the virtual client computing (VCC) market, expanded as a result of the emergence of hybrid work. Hybrid work, defined as a combination of asynchronous, aspatial, and automated styles of achieving outcomes, is in turn a response, most obviously, to global events but more inevitably to the exponential rise in complexity related to technology.

That's an analyst's way of saying that the way we work has permanently changed. We no longer need to work together in time or in space to collaborate, and our automation technologies take care of many tasks we did in the past. Meanwhile, data, interconnection between applications, and applications themselves expanded on an exponential curve, outstripping our ability to remember passwords let alone how to do our own jobs.

Vendors in the ECC ecosystem, including those who offer application streaming and enterprise browsers, rose to this emerging challenge. Some created focused, effective solutions, which work best in cooperation with others. Some wove together consolidated platforms, which cover the entire constellation of needed services, with varying degrees of success.

At the same time, the "AI revolution," which had been boiling since 2015, finally erupted into the public consciousness with the release of ChatGTP and other large language models (LLMs) toward the end of 2022. These technologies promise a world in which individuals no longer interact directly with applications or desktops at all, instead asking for the "computer" do everything for them. Hype aside, there is a great deal to unpack in an era where applications, AI models and the packaged parameters to access them (AI apps), and humans interact in a digital workspace.

Application Streaming and the ECC Ecosystem

Application streaming is, itself, a constellation of technologies related to the encapsulation and delivery of an application or a group of applications to a managed or unmanaged device. It uses some form of concentrator or brokering technology to provide the application as a "stream" to the user, rather than installing the application locally. These technologies are distinguished by applying policy at the concentration layer, by requiring applications to pass through that layer, and may have an optimized protocol for delivering the application, which helps smooth out network or other issues.

Application streaming is used in cases including remote application access, application compatibility management, and the presentation of applications requiring historical operating systems to function. They incorporate features like data loss protection, real-time user monitoring, and infrastructure management.

Enterprise Browsers and the ECC Ecosystem

Enterprise browsers are an evolution of secured browser technology, which got its start as early as 1995. They allow for client-side application of security policy, which may be set centrally or aggregated from multiple sources. The vendor either incorporates these capabilities directly into the browser or deploys them as an add-on to the end-user device's existing browser installation.

Enterprise browsers are used in cases where the enterprise primarily or entirely uses web-enabled applications (including SaaS), already has another zero trust solution, or as one part of the ecosystem of security solutions intended to deal with the expanded threat surface associated with hybrid work.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors were selected for this IDC MarketScape based on the following criteria:

- Operate and have clients in more than one geographic market (Americas, EMEA, Asia/Pacific, etc.)
- Provide application and/or enterprise browser support directly to customers
- Provide the ability to interact with hybrid (private and public cloud) architectures
- Have developed an ecosystem of partnerships enhancing operational and endpoint functionality
- Have an extended market presence, sufficient to indicate they can sustain a mission-critical technology system for at least five years

The points provided in the two bullet points at the end of the list are important, particularly for enterprise technology buyers. Application streaming and enterprise browsers are one part of an ecosystem of technologies used to deliver core business functionality — they must be able to connect the presented application to any peripherals they need and must provide consistent, effective functionality for the duration of the system's deployment. Neither of these is possible when the providing company is financially unstable.

ADVICE FOR TECHNOLOGY BUYERS

Application streaming and enterprise browsers both address the broad functionality of encapsulating, protecting, and projecting applications to end-user devices. They go about this in very different ways, though, with somewhat different resulting functionality. In preparation for using these technologies as part of the enterprise's broader ECC strategy, consider the following:

- **Assess the variance within the user population.** Although it is easy to think that all end users are alike, the acceleration of hybrid work created an ever-increasing variance between end-user needs. Group users not just by job function but by how often they access internally developed and maintained applications, how many software-as-a-service applications they need, and to what extent they interact with a broad array of business-to-business services.
- **Decide whether you need to treat this decision as an "employee as a service" rather than as software**. With software, you intend to devote your own resources, either to administer or to host. With an "employee as a service," you expect to provide an outcome (a digital workspace) with minimal oversight from you or your own resources. This decision needs to cover the entire life cycle of the purchase — it is not enough to have a "lightweight" operating system and "secured"
- **Define what you mean by security, endpoint security, and application security.** The nebulous concepts run rife through the marketing and technical materials presented by vendors — clarity on what you mean will assist you in making reasonable selections among the various offerings
- **Review your existing employees who handle end-user computing and employee experience to determine whether they can be better deployed elsewhere.** For each redeployed resource, assume that their current technical functions will be handled as an "employee as a service"; given the current talent shortage, hiring a lower-cost resource to do the work has a low-probability of success

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

AWS

AWS is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

Amazon Web Services (AWS) offers application streaming and can be used to offer browser isolation technologies but does not offer a unique enterprise browser. These can be accessed through a variety of methods including a web client and managed using either standard AWS or custom-built tools. In addition, Amazon Q provides some ChatOps functionality across the broader Amazon ecosystem.

Strengths

AWS' solutions benefit from their global footprint, comprehensive security framework, and integration with a broad and well-used ecosystem.

AWS' application streaming ecosystem of services benefits from AWS' global footprint, with availability in many of Amazon's global regions and availability zones. This infrastructure enables enterprises to deploy streaming solutions closer to end users, reducing latency and improving performance while maintaining compliance with regional data sovereignty requirements.

They complement this focus on data sovereignty with a defense-in-depth security across their application streaming portfolio, incorporating AWS' robust security capabilities. AWS' solutions feature granular identity management, network isolation, and end-to-end encryption. This is enhanced by continuous compliance monitoring and automated security patching, providing enterprises with a secure foundation that meets stringent regulatory requirements.

The service also benefits from the familiarity that developers and platform teams have with AWS' ecosystem of services. Combined with the concentration of enterprise applications being developed in and around AWS' ecosystem, this allows them to deliver highly responsive and highly resilient streaming experiences with limited need for external integrations.

Challenges

Despite AWS' strong position in the application streaming market, potential customers should consider several challenges when evaluating the company's offerings including the consumption-based pricing model, a self-service approach customer support, and some indications of challenges with Windows-based graphically intense applications.

AWS' consumption-based pricing model, while flexible, introduces complexity for enterprises accustomed to predictable licensing costs. The multidimensional pricing factors — including instance types, usage duration, and additional service integrations

— can make budget forecasting challenging. Organizations without dedicated cloud cost management expertise may struggle to optimize spending and could experience unexpected cost fluctuations during usage spikes.

In keeping with its "builder-first" approach, AWS' support model emphasizes self-service resources and technical documentation over dedicated account management. While premium support tiers are available, they represent significant additional investment. Organizations transitioning from vendors with high-touch support models may find AWS' approach insufficient for complex enterprise deployments, particularly during initial implementation phases.

Some benchmarks and user feedback indicate AWS' solutions may deliver inconsistent user experiences for graphics-intensive Windows applications. Organizations with demanding visualization workloads or legacy Windows applications may encounter optimization challenges that require additional engineering resources to resolve, potentially extending deployment timelines. This feedback did not extend to Linux workloads, which are a particular focus for the vendor.

Consider AWS When

Amazon is suitable for enterprises with existing AWS investments seeking to extend their cloud strategy to application delivery. The ideal customer has technical sophistication to navigate AWS' service ecosystem, values infrastructure flexibility over simplified management, and prioritizes global scalability. Organizations with variable workloads benefit most from Amazon's consumption-based model, particularly those with developer-centric IT operations comfortable with API-driven automation and self-service capabilities. Furthermore, Linux workloads, especially graphics-intensive Linux workloads, seem to perform well. Companies requiring minimal latency for global users will appreciate Amazon's unmatched geographic distribution of streaming infrastructure.

Cloud Software Group (Citrix)

Cloud Software Group (Citrix) is positioned in the Leaders category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

Citrix is now a business unit of Cloud Software Group — a software conglomerate formed from TIBCO and Citrix in September 2022. The combined company offers a wide range of services including both on-premises and cloud-based applications and desktop virtualization solutions.

Citrix provides application virtualization through its Citrix Platform and an enterprise browser through a partnership with Google.

Strengths

Citrix distinguishes itself in the application streaming and enterprise browser market through its historical experience and technological innovations including its cross-platform experience, comprehensive security architecture, and performance optimization options.

Citrix delivers cross-platform consistency through enterprise browser and Secure Private Access, enabling uniform access to virtual, web, and SaaS applications across diverse environments. The company's platform enforces consistent security policies regardless of device type or location, implementing device posture checks that dynamically adjust access controls and data loss prevention (DLP) measures based on contextual factors. This approach ensures seamless user experience while maintaining enterprise-grade security across the digital workspace ecosystem and extended support for peripheral devices including printing.

Citrix's security architecture and adaptive access controls are based on user identity, device health, network location, and risk scores obtained through partnerships with CrowdStrike and Microsoft Intune. The platform features robust data loss prevention capabilities including keylogger protection, screen sharing restrictions, watermarking, and clipboard controls. Browser content redirection technology enhances security by offloading rendering to local machines while maintaining centralized policy enforcement. This multilayered approach enables organizations to implement zero trust principles while preserving user productivity across managed and unmanaged devices.

In addition to an enterprise browser solution, Citrix's experience in virtual desktop infrastructure led the company to create the HDX protocol, which delivers consistent performance even in challenging network conditions through adaptive acceleration techniques. The protocol intelligently balances server-side and client-side rendering based on available resources and application requirements. Browser content redirection offloads web page rendering to local machines, reducing server load while improving responsiveness for graphics-intensive websites. These optimizations ensure consistent application performance across varying bandwidth conditions, enabling productive remote work even in connectivity-constrained environments.

Challenges

Citrix's position as a platform with both application streaming and enterprise browser functionality allows the company to meet a large number of use cases. Unfortunately, this breath of functionality also comes with a corresponding increase in complexity leading to both implementation and operational considerations.

Citrix has markedly reduced the complexity of its implementations in recent years, but customer feedback and IDC research indicate that they remain complex to install. This difference persists in this IDC MarketScape, with customers noting a plethora of not always well-defined options and uncertainty about what specific terms mean.

Small and medium-sized enterprises also noted that it was not always clear what operational burden is associated with the platform, even in the limited deployment associated with using the application streaming and enterprise browser functionality. It should be noted that none of the surveyed customers used the integration between Chrome Enterprise and Citrix, which may have different complexity parameters than direct deployments.

Consider Cloud Software Group (Citrix) When

Citrix is suitable for large enterprises with complex application portfolios spanning legacy, web, and SaaS applications that require consistent security controls and user experiences. Organizations with challenging network conditions will benefit from Citrix's performance optimization technologies, particularly those with global operations requiring reliable remote access.

Google

Google is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

Google delivers application streaming and enterprise browser capabilities through Chrome Enterprise Premium and Cameyo, its cloud-native virtual application delivery platform. With a focus on simplifying administration while maintaining security, Google's solutions enable organizations to deliver Windows and web applications to any device with an HTML5 browser.

Strengths

Google's application streaming and enterprise browser solutions stand out through several key differentiators that leverage the company's cloud expertise and security-first approach including a simplified administrative experience, focus on using modern web technologies, and deep integration with the company's and other identity infrastructure.

Google has made significant investments to streamline the administrative experience through Chrome Enterprise's intuitive management console and Cameyo's simplified deployment workflows. The platform offers templated DLP rules and Gemini-powered policy suggestions that reduce configuration complexity. Chrome Enterprise requires minimal deployment steps — enrolling browsers needs just one platform policy, and enrollment tokens can be reused for efficient scaling. This approach significantly reduces management overhead compared with traditional application delivery solutions.

Google's approach emphasizes modern web technologies through progressive web applications (PWAs), which provide offline functionality while maintaining the feel of locally installed applications. This strategy enables organizations to deliver applications that integrate with file systems, clipboards, and launchers while respecting DLP controls. By leveraging PWA capabilities, Google creates a bridge between traditional desktop applications and modern web applications, providing a seamless user experience across diverse devices without requiring specialized clients or infrastructure.

Google's solutions integrate seamlessly with identity providers to implement context-aware access controls based on user identity, device status, and network conditions. Chrome Enterprise Premium's security features work in conjunction with identity providers to enforce granular policies, while Cameyo presents as a standard SaaS application within identity management systems. This integration enables organizations to leverage existing identity investments while extending zero trust principles to application delivery, simplifying security management while strengthening protection.

Challenges

Google's unified solution with Chrome Enterprise Premium and Cameyo's application virtualization does face some challenges including just released mobile features and limited native partnerships when dealing with the broad ecosystem of peripherals.

While Google has made progress in extending Chrome Enterprise Premium's security features to mobile platforms, there remains inconsistent feature availability across operating systems. Parity between iOS and Android feature sets is on the road map for the second half of 2025 and may be more in synch going forward.

The second point is more difficult for a full platform (application virtualization and enterprise browser) provider. Many of the applications that make up the digital estate, particularly those in use by the line of business, have specific peripheral requirements. Google's partnership with Citrix is key here; using Google's enterprise technology alongside Citrix's protocols and peripheral support is a powerful combination.

Consider Google When

Google is suitable for organizations already invested in the Google ecosystem seeking to modernize their application delivery strategy with minimal infrastructure requirements. The ideal customer has a predominantly web-based application portfolio looking to bring the remainder of their portfolio into a single, unified delivery system.

Inuvika

Inuvika is positioned in the Contenders category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a specialized virtualization provider, Inuvika delivers Windows and Linux applications to any device through its OVD Enterprise platform. With a focus on simplifying virtualization while reducing total cost of ownership, Inuvika's solution enables organizations to deliver applications through a web portal, dedicated desktop, shared desktop, or as integrated apps on users' local desktops. The platform's Linux foundation and containerization technology provide efficient resource utilization while maintaining security and performance across diverse device ecosystems.

Strengths

Inuvika distinguishes itself in the application streaming and enterprise browser market through several key differentiators that leverage its approach to virtualization technology including a highly cost-effective approach, simplified administrative experience tailored to first-time users, and flexible deployment architecture.

Inuvika's OVD Enterprise platform delivers value through its Linux foundation, which enables more efficient resource utilization compared with traditional VDI solutions. By allowing more users per application server and reducing Windows server license requirements, the platform achieves a total cost of ownership that should be lower than its near peers. This cost efficiency is further enhanced by Inuvika's concurrent user licensing model, which aligns costs with actual usage patterns rather than total user counts, providing significant savings for organizations with shift workers or variable usage demands.

Inuvika has designed OVD Enterprise specifically to streamline virtualization for first-time adoption, featuring a single, easy-to-use administrative console that reduces management complexity. This approach eliminates the need for specialized expertise, lowering the barrier to entry for organizations new to virtualization. The platform's intuitive interface enables IT teams to quickly deploy and manage applications across diverse environments without extensive training, significantly reducing administrative overhead while accelerating implementation timelines.

Inuvika's containerization technology enables deployment flexibility across diverse environments. The platform supports seamless delivery of both Windows and Linux applications to any device through multiple access methods, including web portal, dedicated desktop, shared desktop, or as integrated apps on users' local desktops. This versatility is enhanced by platform-specific clients that optimize the experience across Windows, macOS, Linux, Android, and iOS devices. The solution's adaptability extends to global markets through a reseller network spanning over 60 countries and white-labeled DaaS options from managed SPs and cloud SPs.

Challenges

Despite Inuvika's strong position in the application streaming market, organizations considering the company's solution should be aware of several challenges that may impact implementation success, including comparatively limited analytics available to customers and limited brand recognition — making for a smaller user community.

Inuvika's OVD Enterprise appears to offer basic monitoring and logging capabilities but lacks broad-based analytics and reporting frameworks. It does, however, have a full API that can be used for reporting and can be interfaced with Grafana with a deployable dashboard from the Inuvika installer. While the platform provides comprehensive logging for user and administration sessions, it may not deliver the advanced visualization tools, predictive analytics, or customizable dashboards that organizations increasingly expect for operational intelligence. This limitation could impact an organization's ability to optimize resource allocation, identify usage trends, or generate comprehensive compliance reports without implementing additional third-party analytics solutions.

While Inuvika has established a global reseller network across 60 countries, its market presence and brand recognition remain to be clearly established. This could present challenges for organizations seeking extensive implementation support, community resources, or ecosystem integrations. The smaller user community might result in fewer third-party integrations, implementation partners, or specialized expertise available in certain regions, potentially extending implementation timelines or requiring more internal resources to achieve successful deployments.

Consider Inuvika When

Inuvika is suitable for cost-conscious organizations seeking to implement virtualization without the complexity and expense of traditional VDI solutions. The ideal customer has a mix of Windows and Linux applications they need to deliver across diverse devices, values administrative simplicity over advanced features, and operates primarily in connected environments.

Island

Island is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As an enterprise browser provider, Island delivers security and control capabilities through its purpose-built browser platform. The solution enables organizations to maintain robust security controls while providing seamless access to both web-based and legacy applications.

Strengths

Island distinguishes itself in the application streaming and enterprise browser market through several key differentiators that leverage its browser-centric approach to security including browser-native security controls, strong digital employee experience (DEX) monitoring capabilities, and legacy application integrations.

Island delivers security through browser-native controls and a locally installed service for thick applications. The company's platform enforces data protection policies directly within the browser (and the local Island service for thick applications), including granular copy/paste restrictions, download controls, watermarking, and screenshot prevention. This approach provides consistent security across both managed and unmanaged devices without requiring traditional VPNs or proxies that in turn enable organizations to implement zero trust principles while maintaining a user experience across diverse environments.

Island's DEX capabilities provide visibility into application performance metrics including browser wait time, DNS lookup, TCP/TLS handshake, processing time, download response, and DOM build time. The platform automatically correlates these metrics with user location, device type, and network conditions to identify the root causes of performance issues. This comprehensive monitoring enables IT teams to proactively address application performance problems before they impact productivity.

Island bridges modern and traditional application environments through its built-in connectivity capabilities for non-web resources. The browser includes native RDP, SSH, and SMB clients that enable secure access to legacy applications, command-line resources, and file shares without requiring additional software. This integration creates a unified workspace where users can access both SaaS applications and traditional systems through a single, consistent interface while maintaining robust security controls across all application types.

Challenges

Organizations considering Island's solution should be aware of several challenges that may impact implementation success including limited application streaming capabilities, some limitations in its broader analytics suite, and some complexity issues at scale.

Island's primary focus on browser-based security means it lacks native application streaming capabilities for complex Windows applications with specific dependencies or performance requirements. While the platform can integrate with existing VDI solutions through its built-in RDP client and enforce data protection policies in desktop applications running on the endpoint, organizations with extensive traditional application portfolios may need to maintain separate streaming infrastructure alongside Island. This hybrid approach can increase overall solution complexity and potentially create inconsistent user experiences between browser-native applications and streamed applications.

While Island provides comprehensive digital employee experience monitoring, its broader analytics capabilities appear less mature than specialized analytics platforms. The solution offers visibility into browser-based activities but may lack the sophisticated data correlation, predictive analytics, and customizable reporting frameworks provided by dedicated analytics solutions. Organizations with complex compliance reporting requirements or those seeking advanced user behavior analytics may need to supplement Island's native capabilities with additional tools, potentially increasing overall solution complexity.

Island's implementation in large, complex environments may require significant planning and coordination across multiple teams. The solution's integration with existing identity systems, security tools, and application ecosystems demands careful orchestration, particularly when implementing granular policies across diverse user groups and application types. Organizations with limited browser management expertise may experience extended deployment timelines as they develop the specialized knowledge required to fully leverage Island's extensive policy framework and integration capabilities

Consider Island When

Island is suitable for security-conscious organizations seeking to extend zero trust principles to browser-based work while reducing dependency on traditional VDI solutions. The ideal customer has a significant investment in SaaS applications but still maintains legacy systems requiring secure access, values granular visibility and control over data movement, and needs to support remote work across both managed and unmanaged devices.

Microsoft

Microsoft is positioned in the Leaders category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

With a comprehensive portfolio spanning virtualization, browser security, and cloud services, Microsoft delivers application streaming and enterprise browser capabilities through App-V and Edge for Business. The company's integrated approach leverages its extensive Microsoft 365 ecosystem to provide secure and consistent application experiences across diverse devices while maintaining robust security controls through zero trust architecture and conditional access policies that adapt to user context, device health, and risk signals.

Strengths

Microsoft's application streaming and enterprise browser solutions distinguish themselves through several key differentiators that leverage their ecosystem integration and security-first approach, including exceptional integration into their wider ecosystem, a comprehensive zero trust architecture, and some offline capabilities.

Microsoft's solutions provide integration with the broader Microsoft 365 ecosystem, creating a cohesive digital enterprise platform. Edge for Business integrates natively with Microsoft Entra ID for authentication, Purview for data protection, and Endpoint Manager for device management. This integration enables unified policy management across applications, simplified administration through familiar interfaces, and consistent security controls that span the entire digital workspace, significantly reducing management complexity while enhancing security posture.

Microsoft implements a sophisticated zero trust security model that incorporates user identity, device health, location, and risk signals into access decisions. Edge for Business enforces conditional access policies that can require additional verification factors before accessing organizational resources, even on unmanaged devices. The browser creates distinct profiles with visual differentiation between work and personal browsing, preventing cross-contamination by maintaining separate cookies, cache, and browsing data between contexts, effectively balancing security with user experience.

Challenges

Organizations considering Microsoft's solutions should be aware of several challenges that may impact implementation success, including limited analytics extensibility, complex licensing structures, and integration limitations outside of the company's own ecosystem.

Microsoft's analytics capabilities, while functional for basic monitoring, lack the extensibility offered by specialized analytics platforms and the detail provided by specialized providers. App-V provides basic usage reporting through PowerShell commands that display package usage statistics but lack comprehensive visualization tools or customizable dashboards. Edge for Business offers more detailed metrics through Microsoft Endpoint Manager, but the platform's ability to export this data for integration with third-party analytics systems is limited, potentially creating visibility gaps for organizations with complex reporting requirements or existing investments in specialized monitoring tools.

Microsoft's licensing model for application streaming and browser management can be challenging to navigate, particularly for organizations without dedicated Microsoft licensing expertise. The various subscription levels, add-on features, and dependencies on other Microsoft products create complexity in determining the most cost-effective approach. Organizations frequently struggle to align licensing purchases with actual usage patterns, which eventually leads to either over-provisioning or unexpected costs when scaling. This complexity extends to understanding the full economic impact when implementing these solutions alongside existing Microsoft investments.

While Microsoft's solutions excel within its ecosystem, organizations with diverse technology stacks may encounter integration challenges. Edge for Business provides some API access for customers to extract usage data or integrate with non-Microsoft security tools. Organizations heavily invested in alternative identity providers, endpoint management systems, or security platforms may find that Microsoft's solutions require additional configuration or custom development to achieve the same level of integration provided natively within the Microsoft ecosystem, potentially increasing implementation complexity and ongoing management overhead.

Some of these challenges may be addressed as part of Microsoft's recently announced connector program.

Consider Microsoft When

Microsoft is suitable for organizations already invested in the Microsoft 365 ecosystem seeking to extend their security and management capabilities to application delivery. The ideal customer has a mix of modern web applications and legacy Windows applications requiring consistent security controls across diverse devices and work locations.

Omnissa

Omnissa is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

Omnissa delivers application streaming and enterprise browser capabilities through its integrated Omnissa platform that includes Omnissa Horizon, App Volumes, and Workspace ONE. With Omnissa digital employee experience customers can optimize user experience while maintaining robust security. Omnissa enables organizations to deliver and manage applications across diverse environments leveraging AI-driven analytics and automation that proactively identifies and resolves performance issues before they impact productivity.

Strengths

Omnissa distinguishes itself in the application streaming and enterprise browser market through several key differentiators that leverage the company's comprehensive platform approach and focus on user experience, including experience management, a comprehensive zero trust framework, and extensive ecosystem integration.

Omnissa Horizon offers secure delivery of virtual apps and desktops, with flexible and scalable deployment options ranging from on-premises to multicloud. Granular security policies allow IT to securely deliver apps to virtual and physical endpoints while providing a consistent and seamless end-user experience. To support various use cases like distributed workforces, BYOD, and compliance, IT can use Horizon to publish apps or deliver through VDI or DaaS. Omnissa also offers App Volumes that equips IT with a real-time app delivery and full life-cycle management solution for digital workspaces. Using a unique "on demand" delivery approach that supports any Windows app, App Volumes streamlines app management across virtual and physical endpoints. App Volumes with Apps on Demand delivers an app when the user clicks on it, reducing infrastructure costs while limiting attack surfaces when an app vulnerability arises.

Omnissa's Experience Management provides visibility into application performance through AI-powered analytics that automatically identify root causes of user experience issues. The platform collects metrics across the entire delivery chain — including device health, application performance, and network conditions — correlating these factors to pinpoint performance bottlenecks. This proactive approach enables IT teams to resolve issues before users report them, significantly reducing mean time to resolution while improving overall productivity through consistent application performance.

Omnissa's app catalog (Workspace ONE Intelligent Hub) and access broker (Omnissa Access) work together to incorporate multiple contextual factors into access decisions. The company's platform evaluates device enrollment status, network conditions, user behavior patterns, and location to create risk-based conditional access policies. This approach enables organizations to implement least-privilege access principles while maintaining productivity across diverse work environments. The integration with Omnissa's Trust Network further enhances security by incorporating signals from third-party security tools into access decisions, creating a unified security framework across the digital workspace.

Omnissa provides integration capabilities across identity providers, endpoint management systems, and security tools through its Omnissa platform. The platform enables single sign-on to web, SaaS, mobile, and legacy applications through Omnissa

Access while maintaining consistent security controls through SAML authentication. This integration ecosystem allows organizations to leverage existing investments in security and management tools while extending consistent policies across all application types, significantly reducing administrative overhead while strengthening overall security posture.

Challenges

Organizations considering Omnissa's solutions should be aware of several challenges that may impact implementation success, including issues around implementation and change management complexity.

Omnissa's comprehensive feature set introduces significant implementation complexity that require specialized expertise to fully leverage. Customer feedback indicates that organizations often underestimate the technical knowledge needed to architect optimal solutions across Omnissa's extensive portfolio. The platform's multiple management consoles and configuration points require careful planning for authentication flows, policy configurations, and integration with existing security infrastructure.

While Omnissa provides robust capabilities across device types — including mobile — organizations may face challenges with user and administrator adoption due to the breadth and depth of the platform. The transition to unified endpoint and application management, especially in large enterprises with entrenched legacy systems and processes, can require significant change management efforts. Ensuring that staff are adequately trained and that workflows are adapted to leverage Omnissa's full capabilities may extend rollout timelines and require additional investment in enablement and support resources.

Consider Omnissa When

Omnissa is suitable for medium-sized to large enterprises with complex application portfolios seeking to unify management across traditional, web, and mobile applications through a single platform. The ideal customer has existing virtualization expertise or resources to invest in specialized skills, values comprehensive analytics and automation capabilities, and requires sophisticated security controls that adapt to diverse access scenarios.

Palo Alto Networks

Palo Alto Networks is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a large cybersecurity provider, Palo Alto delivers enterprise browser capabilities through its Prisma Access Browser, which can be deployed standalone or as an extension of a SSE solution. The solution is currently available as a component of Palo Alto Networks' SASE platform, which includes everything from core security functions to software supply chain management. The solution enables organizations to secure browser-based work environments across both managed and unmanaged devices while maintaining consistent security controls for all SaaS and web applications.

Strengths

Palo Alto Networks' enterprise browser solution stands out through several key differentiators that leverage the company's security expertise and cloud-native architecture, including advanced web security and data protection, browser isolation, identity security, native integration into a broader SASE framework, application acceleration, and an interesting proposition around composed agentic applications.

Prisma Access Browser integrates natively with Palo Alto Networks' broader SASE platform, creating a unified security framework across all access scenarios. This integration enables consistent policy enforcement regardless of device management status or location while leveraging the platform's AI-powered threat detection, antiphishing, and analysis capabilities. In particular, organizations will benefit from simplified administration through a single policy framework that extends across the zero trust, browser, and application security.

Prisma Access Browser incorporates SASE's App Acceleration capability to improve application performance. The platform employs predictive modeling of user and application behavior to anticipate interactions and pre-fetch dynamic content, maintaining responsiveness even in challenging network conditions. This optimization approach ensures consistent user experiences across diverse connectivity scenarios while maintaining robust security controls, enabling productive remote work without compromising on protection or performance.

The combination of Prisma Access Browser's security infrastructure integrations along with its approach to data loss protection and performance optimization gives Palo Alto Networks an interesting set of capabilities around agents and composed agentic applications. In the short term, this manifests as the ability to control data loss around GenAI tools, including direct agents and applications built with some GenAI capabilities. In the medium term, this will likely expand to include the securing and acceleration of applications composed "in the moment" through the interaction of agents and various agent-adjacent technologies.

Challenges

Despite Palo Alto Network's strong position in the enterprise browser market, organizations considering the company's solution should be aware of several challenges that may impact implementation success, including some challenges with endpoint and application analytics maturity and implementation complexity when not undertaken as part of a larger effort.

While Prisma Access Browser provides useful security metrics, including application risk scores, its digital employee experience capabilities could use improvement. In particular, organizations with complex compliance reporting requirements or those seeking advanced user behavior analytics may need to supplement Palo Alto Networks' native capabilities with additional tools, potentially increasing overall solution complexity.

Palo Alto Networks' customers can leverage Prisma Access Browser as part of a larger Palo Alto Networks platform. Deploying it in a standalone mode is possible but less compelling from a features standpoint and may introduce needless complexity into an already overly chaotic environment. Customers cited this as particularly problematic when engaged in larger organizational change activities, likely as a result of a shift in operational responsibility between the security, platform, and digital employee experience teams.

Consider Palo Alto Networks When

Palo Alto Networks is suitable for security-focused organizations seeking to implement zero trust principles for browser-based work across both managed and unmanaged devices. The ideal customer has significant investments in SaaS applications, values consistent security controls regardless of device ownership, and has sufficient IT resources (developers, security, and operations) to gain value from the integrated platform. Smaller or less well-staffed organizations will still benefit but may not be able to get everything possible from the platform.

Parallels

Parallels is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

Parallels delivers application streaming capabilities through its Parallels Remote Application Server (RAS) platform and Parallels DaaS and secure browsing through Parallels Browser Isolation. The solution enables organizations to deliver Windows applications and secure browser-based access across diverse device ecosystems while maintaining robust security controls. With a focus on simplicity and flexibility, Parallels provides a unified workspace experience that bridges traditional applications and modern web resources.

Strengths

Parallels distinguishes itself in the application streaming and enterprise browser market through several key differentiators that leverage the company's innovative approach to virtualization and security, particularly in its administrative experience, offline experiences through Parallels Desktop, and a flexible deployment architecture.

Parallels has designed its platform to minimize management complexity through intuitive interfaces and automation capabilities. The RAS Console provides centralized control with wizard-driven workflows that streamline application deployment through a four-step setup process completed in under ten minutes. Administrators can automatically scan session hosts for installed applications, eliminating manual path configuration. This approach significantly reduces administrative overhead while accelerating implementation timelines, making the solution particularly valuable for organizations with limited specialized IT resources.

Alongside online use cases where compute on device is crucial (e.g., for developers and knowledge workers), Parallels delivers offline functionality through Parallels Desktop, which provides a hypervisor on client devices — making applications available locally without internet dependency. The platform supports integration of local applications directly through Parallels Client while implementing disk encryption using AES-256. Smart virtual disk access technology only decrypts accessed portions in real time, maintaining security while enabling productivity in disconnected environments. This capability ensures business continuity for mobile workers and those in connectivity-challenged locations.

Parallels offers remarkable deployment versatility across diverse environments, supporting multiple hypervisors and cloud platforms including Azure and Amazon. The solution provides a low-cost integration platform that spans datacenters and edge locations while offering an opinionated DaaS solution on Azure. Parallels' flexibility extends to access methods through a secure gateway that translates RDP streams into HTML5 for browser access. The platform's multitenant architecture further enhances this adaptability, making it suitable for service providers and organizations with complex deployment requirements.

Challenges

Organizations considering Parallels' solutions should be aware of several challenges that may impact implementation success. These challenges include:

- Parallels has not yet fully integrated AI-based operations tools beyond autoscaling, image optimization, and power scaling. While the platform is fully API enabled, allowing organizations with existing automation teams to integrate Parallels into their workflows, the lack of native AI-driven capabilities may create disadvantages. Organizations seeking sophisticated predictive analytics or automated remediation capabilities may need to implement additional third-party solutions to supplement Parallels' native functionality.
- Unlike other hybrid platforms, Parallels does not currently offer a native or opinionated endpoint management solution. This limitation may create integration challenges for organizations seeking a comprehensive workspace solution that includes device management capabilities. While Parallels can integrate with third-party endpoint management tools, the additional complexity and potential gaps in this integration may extend implementation timelines and increase total cost of ownership for organizations with diverse device ecosystems.
- Some customers have noted a lack of clarity about which Parallels solutions meet specific use cases. This confusion appears to be a side effect of numerous recent product launches, including an edition to the Parallels Desktop product line. Organizations may struggle to identify the appropriate combination of Parallels offerings for their specific requirements, potentially leading to suboptimal implementations or unnecessary licensing costs. Without clear guidance on solution mapping to business needs, customers may face challenges in maximizing their investment in the Parallels ecosystem.

Consider Parallels When

Parallels is suitable for small and medium-sized businesses and midmarket enterprises with multiple complex use cases and limited specialized IT staff. The ideal customer values administrative simplicity, deployment flexibility across diverse environments, and cost-effective virtualization solutions. Organizations with shift workers will particularly benefit from Parallels' concurrent user licensing model, which aligns costs with actual usage patterns rather than total user counts.

SERAPHIC

SERAPHIC is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a browser security specialist, SERAPHIC delivers enterprise browser capabilities through its lightweight agent technology that secures browsing sessions without compromising user experience. The platform enables organizations to enforce consistent security policies across managed and unmanaged devices while maintaining native browser experiences. With a focus on unobtrusiveness and performance, SERAPHIC helps enterprises protect sensitive data and enforce compliance requirements across diverse browser environments, as well as SaaS applications and private applications without requiring complex infrastructure.

Strengths

SERAPHIC distinguishes itself in the enterprise browser market through several key differentiators that leverage their innovative approach to browser security. These differentiators include a nondisruptive security architecture, flexible deployment options, and advanced browser threat detection.

SERAPHIC's lightweight agent technology delivers security without compromising user experience or requiring browser replacement. The platform injects JavaScript security controls into existing browsers rather than replacing them, preserving familiar interfaces while adding enterprise-grade protection. This approach eliminates user resistance to adoption typically associated with new browser deployments, accelerating implementation timelines while maintaining robust security controls across Chrome, Edge, Firefox, and Safari environments.

SERAPHIC provides deployment flexibility through multiple implementation methods including browser extension, dedicated browser, or proxy-based approaches. This versatility enables organizations to select the optimal deployment strategy based on their specific security requirements, existing infrastructure, and device management capabilities. The platform's ability to secure browsing sessions across managed and unmanaged devices without requiring device management makes it particularly valuable for organizations with complex BYOD environments or third-party access requirements.

SERAPHIC delivers protection against browser-specific threats through its specialized security focus. The platform prevents attacks including browser exploitation, man-in-the-middle attacks, and malicious extensions while providing runtime protection against emerging threats. This browser-centric security approach addresses vulnerabilities that traditional security tools often miss, creating an additional defensive layer that complements existing security investments while protecting the increasingly critical browser attack surface.

Challenges

SERAPHIC's unique enterprise browser architecture allows the company a large degree of flexibility in deployment and implementation. However, they have some notable challenges related to third-party device integrations and complex analytics.

In particular, SERAPHIC does not address concerns with third-party device integration, a key feature for broader deployments. This is less of a concern for enterprises that rely largely on contemporary SaaS offerings but is problematic for enterprises of any scale who have deployed IoT systems, printers, or even just headphones at scale. This issue can be addressed through the use of additional tools but at a cost of increasing complexity.

SERAPHIC's analytics for in-browser applications are comparable with other enterprise browser solutions but lack the sophistication. It would benefit from additional integrations with dedicated digital employee experience vendors apps as well as more comprehensive predictive analysis around device and application interactions, possibly extending into third-party device management.

Consider SERAPHIC When

SERAPHIC is suitable for security-conscious organizations seeking to enhance browser security without disrupting user experience or replacing existing browsers. The ideal customer has a significant investment in web-based applications, values deployment flexibility across diverse environments, and needs to secure browsing sessions on both managed and unmanaged devices. Organizations with BYOD programs or third-party access requirements will particularly benefit from SERAPHIC's ability to enforce security policies without requiring device management.

v2 Cloud

v2 Cloud is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a desktop virtualization provider focused on small to medium-sized businesses, v2 Cloud delivers Windows-based virtual desktops accessible from any device through its cloud workspace platform. With an emphasis on simplicity and affordability, v2 Cloud enables organizations to centralize application management while providing secure remote access to business resources. v2 Cloud's solution eliminates the need for complex infrastructure management while maintaining robust security through centralized data storage and encrypted remote display protocols.

Strengths

v2 Cloud distinguishes itself in the application streaming market through several key differentiators that address the specific needs of small to medium-sized businesses including ease of use, administrative analytics capabilities, and deployment versatility.

v2 Cloud delivers ease of use through its simplified management console designed specifically for organizations with limited IT resources. The platform features preconfigured application templates and automated deployment workflows that enable rapid workspace provisioning without specialized expertise. This approach significantly reduces implementation complexity and ongoing management overhead, allowing organizations to deploy and maintain virtual workspaces without dedicated virtualization specialists.

v2 Cloud provides analytics capabilities that enable administrators to optimize resource allocation and control costs. The platform tracks detailed metrics including CPU utilization, memory usage, storage performance, and application response times across user segments. These insights help identify resource bottlenecks, underutilized instances, and usage patterns by department or location. The system correlates metrics to identify optimization opportunities, providing recommendations for rightsizing resources and implementing schedule-based provisioning aligned with actual business hours.

v2 Cloud offers deployment versatility through its multitenant cloud architecture that supports diverse business requirements. The platform enables white-label capabilities for managed service providers while maintaining regional datacenters to address compliance requirements. This flexibility extends to customization options that allow organizations to replace the v2 Cloud logo with their company branding, customize color schemes, and add personalized messaging across the management console, log-in portal, and desktop environment, creating a consistent brand experience for end users.

Challenges

Despite v2 Cloud's strong position in the desktop virtualization market, organizations considering its solution should be aware of several challenges that may impact implementation success, including a lack of granular application streaming options, requirements for continuous network access, and geographic limitations for international buyers.

v2 Cloud's primary focus on full desktop virtualization means it lacks the granular application streaming capabilities. While the platform excels at delivering complete Windows desktop environments, organizations seeking to stream individual applications without the overhead of full desktops may find the solution less efficient. This limitation could impact resource utilization and user experience for scenarios where only specific applications need to be delivered rather than complete desktop environments.

v2 Cloud's architecture requires continuous network connectivity for application access, with limited support for offline work scenarios. The solution's reliance on remote display protocols means that applications and data remain in the cloud, with only compressed and encrypted images transmitted to end devices. While this approach enhances security, it creates productivity challenges for users in disconnected environments or locations with unreliable internet connections, potentially impacting organizations with mobile workforces or field operations.

v2 Cloud's primary focus on North America and Europe may present challenges for global organizations requiring consistent performance across diverse regions. While the platform maintains regional datacenters to address compliance requirements, its presence in emerging markets appears more limited. Organizations with significant operations in Asia/Pacific, Latin America, or Africa may experience performance variations or compliance challenges when implementing v2 Cloud across these regions.

Consider v2 Cloud When

v2 Cloud is suitable for small to medium-sized businesses (5–500 employees) seeking to implement desktop virtualization without the complexity and expense of traditional VDI solutions. The ideal customer has limited IT resources, values administrative simplicity over advanced features, and requires secure access to Windows applications from diverse devices.

Workspot

Workspot is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a cloud-native digital workspace provider, Workspot delivers virtual desktops and applications through its Global Desktop technology that places computing resources in cloud regions closest to users. With a focus on performance optimization and user experience, the platform enables organizations to securely deliver Windows applications and browser-based resources across diverse devices while maintaining centralized security controls through a unified management interface that simplifies administration and monitoring.

Strengths

Workspot distinguishes itself in the application streaming and enterprise browser market through several key differentiators that leverage Workspot's cloud-native architecture and performance-focused approach, including performance optimization, digital experience monitoring, and a well-architected zero trust security framework.

Workspot's cloud-native architecture delivers excellent performance by strategically placing virtual desktops in cloud regions closest to users. The platform supports high-performance 3D CAD applications by centralizing data and compute in optimal cloud regions while leveraging high-bandwidth cloud backplanes (1Gbps) and low-latency local networks. This approach ensures responsive application experiences even for graphics-intensive workloads, while the platform's adaptive H.264-based protocol automatically adjusts to available bandwidth conditions to maintain consistent performance across varying connectivity environments.

Workspot Trends provides visibility into application performance through detailed metrics collection, including CPU/memory usage, network conditions, round-trip time, and user satisfaction ratings. The platform enables administrators to optimize cloud infrastructure costs and to compare performance between desktop pools to identify specific conditions causing issues, while the Workspot Watch real-time dashboards display user experience and server metrics. This data-driven approach, assisted by AI and machine learning, enables IT teams to quickly identify and resolve performance problems, significantly reducing mean time to resolution while improving overall productivity.

Workspot implements a well-architected zero trust security model that incorporates user attributes, device posture checks, and location data into access decisions. The platform enforces different authentication requirements for different gateways, ensuring consistent security across both managed and unmanaged devices. Organizations can integrate Workspot with networking security from Zscaler, f5, and Palo Alto Networks. Multilayer encryption protects data both in transit and storage, while integration with security tools like CyberArk enhances protection against unauthorized access, brute force attacks, and IP spoofing. This comprehensive approach enables organizations to implement least-privilege access principles while maintaining productivity.

Challenges

Despite Workspot's strong position in the application streaming and enterprise browser market, organizations considering Workspot's solution should be aware of several challenges that may impact implementation success, including limitations in the extensibility of their analytics framework, a need to integrate with more management tools, and some challenges with offline access.

While Workspot provides performance monitoring through Workspot Trends, the platform's analytics capabilities may not meet all customer platform requirements. The solution integrates with SIEM systems like Splunk, Exabeam, Elastic, and Azure Sentinel, through its API, collecting metrics, logs, and traces every 30 seconds, but may lack the sophisticated data correlation, predictive analytics, and customizable reporting frameworks offered by more mature solutions. Organizations with complex compliance reporting requirements or those seeking advanced user behavior analytics may need to supplement Workspot's native capabilities with additional tools.

Workspot's platform enables organizations to use any existing security tools like FireEye, CrowdStrike, and SentinelOne; however, its integration capabilities with existing security and management tools appear more limited. While the platform connects to conditional access systems and reports posture actions and connection details for each user session, it relies on organizations to use its API to integrate the data into a SIEM. Organizations with complex technology environments may face challenges integrating Workspot with their full range of security tools, analytics platforms, or management systems. This integration complexity could extend implementation timelines and increase total cost of ownership for organizations with diverse application portfolios and established security ecosystems.

Consider Workspot When

Workspot is suitable for organizations seeking to implement cloud-native virtual desktops and application streaming without the complexity of traditional VDI solutions. The ideal customer values performance optimization for graphics-intensive applications, requires global deployment capabilities with regional data residency, and needs to support both managed and unmanaged devices through a unified security framework. Engineering firms, architecture companies, and manufacturing organizations will particularly benefit from Workspot's ability to deliver high-performance 3D applications to any device, while companies with distributed workforces will appreciate the platform's ability to place computing resources in cloud regions closest to users.

Zscaler

Zscaler is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide application streaming and enterprise browsers vendor assessment.

As a zero trust security provider, Zscaler delivers enterprise browser capabilities through its zero trust browser and privileged remote access solutions, which extend its comprehensive SASE platform. With a focus on securing browser-based work environments without requiring endpoint management, Zscaler enables organizations to implement consistent security controls across both managed and unmanaged devices while providing detailed visibility into application performance and user experience through its digital experience monitoring platform.

Strengths

Zscaler distinguishes itself in the enterprise browser market through several key differentiators that leverage their security expertise and cloud-native architecture including granular contextual access policies integrated into its zero trust exchange architecture while providing contextually aware application performance monitoring.

Zscaler's Zero Trust Exchange enforces granular access policies based on multiple contextual factors including user identity, device posture, location, application type, and risk level. The platform dynamically applies these policies using AI-driven analytics and integrated identity providers, creating an adaptive security model that adjusts protection based on real-time risk assessment. This approach enables organizations to implement least-privilege access principles while maintaining productivity across diverse work environments, significantly reducing the attack surface while allowing appropriate access to business resources.

Zscaler's platform delivers accelerated performance through its Zero Trust Exchange architecture, which optimizes application delivery while maintaining robust security controls. The recently developed Turbo Mode for zero trust browser achieves up to 50fps using WebGL instruction sets processed by local device GPUs rather than streaming pixels, creating a responsive user experience even for graphics-intensive applications. This optimization approach ensures consistent application performance across varying network conditions while maintaining security boundaries between personal and work activities.

Zscaler's ZDX platform provides visibility into application performance through AI-powered diagnostics that precisely identify root causes of performance issues. The system isolates problems across the entire delivery chain — including devices, Wi-Fi, networks, and applications — while providing actionable insights for resolution. By tracking comprehensive metrics such as page fetch times, DNS resolution times, network latency, and UCaaS call quality, ZDX enables IT teams to proactively address performance bottlenecks before they impact productivity, significantly reducing mean time to resolution.

Challenges

Despite Zscaler's strong position in the enterprise browser market, organizations considering Zscaler's solution should be aware of several challenges that may impact implementation success including limitations in offline capabilities, a highly variable implementation complexity, and challenges with ecosystem integration.

Zscaler's browser solutions are intended to be used in conjunction with other Zscaler SASE and SSE products. Most organizations using Zscaler browser solutions use other Zscaler products. Deploying Zscaler browser solutions as a component of other Zscaler SASE and SSE solutions is very easy, even for organizations with limited specialized security expertise. But organizations trying to integrate Zscaler browser solutions into another vendor's SASE or SSE products may find this complex with too many other overlapping capabilities.

While Zscaler provides robust integration with major identity providers and security tools, organizations with diverse technology stacks may encounter integration challenges with specialized or legacy systems. The platform's OneAPI initiative aims to address this through a unified API framework, but organizations with complex existing technology ecosystems including multiple generations of peripherals may still face challenges achieving seamless integration across all components. This limitation could potentially increase implementation complexity and ongoing management overhead for organizations with significant investments in specialized security or management tools that fall outside Zscaler's primary integration partnerships.

Consider Zscaler When

Zscaler is suitable for security-focused organizations seeking to implement zero trust principles for browser-based work across both managed and unmanaged devices. The ideal customer has significant investments in SaaS applications, values consistent security controls regardless of device ownership, and already has an existing Zscaler implementation.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users.

Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

The application streaming and enterprise browser market comprises software solutions enabling secure, managed access to web/SaaS applications and legacy desktop applications across distributed workforces. Unlike consumer-grade browsers, these enterprise-focused platforms integrate directly with identity providers, device management systems, and security infrastructure to deliver contextual access controls.

The application streaming submarket focuses on enabling on-demand access to software via a concentrator or broker, while enterprise browsers provide a policy-enforced environment for web app interactions. Together, these technologies address critical challenges in hybrid workforces, SaaS adoption, and zero trust architecture in a lighter-weight way than either desktop-as-a-service or full VCC stacks.

Strategies and Capabilities Criteria

Company strategies were assessed for doctrinal alignment and internal consistency, alignment with expected market trends over the next five-year period as detailed in IDC FutureScape documents, and the ability to adapt to unanticipated changes. The company's concept of the evolving digital workspace was assessed separately from the core VCC strategy. The vendor's previous answers to strategy questions from prior VCC/DaaS IDC MarketScape documents were reviewed for consistency, evolution, and the ability to deliver planned functionality. Customer feedback was taken into consideration as well.

Product capabilities were assessed for completeness and competence of core functionality, completeness and competence of extended functionality, and alignment with *IDC TechScape: Worldwide Virtual Client Computing, 2018* (IDC #US44416918, November 2018). The capabilities were also adjusted based on functional, implementation, and operational feedback from both vendor and customer interviews (see Tables 1 and 2).

TABLE 1

Key Strategy Measures for Success: Worldwide Application Streaming and Enterprise Browsers

Strategies Criteria	Definition	Weight (%)
Functionality or offering strategy	▪ There is a road map based on customer and partner input that covers part of cloud, data analysis, mobility solutions, and social integration. ▪ The vendor is making discrete steps to meet defined future-looking scenarios.	35.00
Financial/funding	▪ The vendor sees consistent growth, or increase, in market share.	15.00
Delivery	▪ The vendor provides an appropriate level of complexity for meeting the defined use cases.	15.00
Innovation	▪ The vendor expresses its innovation strategy well enough that customers understand it and it meets their specific needs.	20.00
Growth	▪ The vendor possesses targeted vertical solutions along with the ability to support those solutions across a wide range of clients while also providing appropriate support for all customers.	15.00
Total		100.00

Source: IDC, 2025

TABLE 2

Key Capability Measures for Success: Worldwide Application Streaming and Enterprise Browsers

Capabilities Criteria	Definition	Weight (%)
Functionality or offering	▪ The vendor demonstrates its ability to offer specific capabilities listed.	15.00
Pricing model or structure of product/offering	▪ The vendor has a pricing model for different types of delivery.	10.00
Other	▪ The vendor provides and integrates with both analytic and compliance tools for operational and security requirements. ▪ The vendor's solution provides methods for managing the user experience across multiple platforms. ▪ The vendor provides support for developers to expand and extend its solution. ▪ The vendor provides tools to remediate and improve on the user experience, not limited to times when it is degraded. ▪ The vendor addresses specific security concerns with its solution.	60.00
Portfolio benefits	▪ The vendor maintains a dedicated ecosystem of technology and service partnerships that allow it to maintain technical compatibility with key infrastructure systems.	15.00
Total		100.00

Source: IDC, 2025

LEARN MORE

Related Research

- *Worldwide Virtual Client Computing Software Forecast, 2025–2029* (IDC #US52397925, June 2025)
- *Market Analysis Perspective: Asia/Pacific Enterprise Automation, 2025* (IDC #AP52923225, June 2025)
- *Agents as Apps: An Opportunity for Greater Innovation, More Revenue, and Increased Market Share* (IDC #US53385925, May 2025)
- *Enterprise Application Customers: Navigating the Challenges of Tariffs, Regulations, and Costs with AI* (IDC #US53386125, May 2025)

Synopsis

This IDC study evaluates vendors in the application streaming and enterprise browsers submarkets, part of the expanding enterprise client computing ecosystem driven by hybrid work and technological complexity. It highlights the shift in work dynamics, emphasizing asynchronous collaboration and automation. Vendors are assessed based on their ability to provide secure, managed access to applications, integrating with identity providers and security systems. The document also includes vendor profiles, strengths, challenges, and criteria for success in this evolving market.

"In a world where hybrid work reshapes our digital landscape, application streaming and enterprise browsers emerge as pivotal players, redefining how we interact with technology. As AI revolutionizes our workspace, the challenge lies in seamlessly integrating these tools to enhance productivity without compromising security. The future beckons a paradigm shift where applications serve us, not the other way around. Are we ready to embrace this transformation and unlock the full potential of our digital ecosystem? As the very meaning of work changes, how, when, where, and with what we work will also change," said Shannon Kalvar, research director, Enterprise Client Platforms at IDC. "Application streaming and enterprise browsers are one part of the industry's response to those changes; one which is very much a work in progress."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.