High Impact Differentiators (Updated 2025-09-29)	Netskope	Cloudflare
Comprehensive Platform and Architecture Driven by Zero Trust Principles		
Global, private, elastic network directly peered with all major cloud service providers without surcharges or exclusions	• Dedicated NewEdge private security network spans 78+ unique true-compute metro regions for globally-optimized, interconnected, and resilient connectivity	• Claims 300+ cities without disclosure on SSE vs. CDN locations • Gartner consistently rates CF as a Niche player with weak capabilities
All user to app traffic makes a single pass through the global private network with real-time inspection and control by a full stack of security services	• No added latency due to third-party cloud provider path inefficiencies • Single pass Zero Trust Engine with no backhauling to deliver security controls	• Supports Single Pass with limited inspection engines • Limited security inspection for data / threats (lowest Gartner SSE CC scores)
Every user connection to global private network offers in-country localized experience, access to geo-fenced content and source IP restricted apps	• All metro regions offer all services to all customers • Localization Zones for 200+ countries & Dedicated Egress IP in every region	• Not every service runs in every PoP • Dedicated Egress IPs supported for select data centers only upon request
End users experience low latency and high availability with all traffic steered through global private network	• Commits to 10ms SLA for non-decrypted and 50ms SLA for decrypted traffic • 99.999% uptime with latency SLA based on 95th percentile	• 100% availability SLA with exclusions and limited service credits • No processing latency SLA which would include security inspection
Deep real-time visibility into and control over user risk and trustworthiness during user sessions	• Continuous Adaptive Trust processed in real time for user, application, device, and data risk signals, including user behavior and application instance	• Limited risk evaluation due to lack of contextual awareness (app, activity, instance, user risk). Focuses on device posture risk as primary risk factor.
Effective Risk Management, Data Protection, and Threat Prevention		
Platform does not require bypass of productivity and SaaS app traffic to maintain acceptable user experience (e.g., MS 365 Outlook, SharePoint)	• Full SSL decryption and inspection of all SaaS traffic including M365 • Addresses the most significant risk, attack surface, and data exfiltration vector	• Require bypassing productivity and SaaS traffic specifically MS product suite • No visibility into attack surface and data exfiltration for bypassed SaaS
Application and user risk scoring utilized for access, threat prevention, data protection, DLP, and UEBA policies	• 80,000+ apps with ~60 risk criteria across key domains to improve TPRM • Advanced UEBA with 125+ ML models to identify insider threats	• Limited app discovery without risk scoring and requires manual app tagging • Very few CASB APIs supported and virtually no UEBA
Real-time control of cloud applications using predefined activities across thousands of applications and millions of websites	• Patented Zero Trust Engine which decodes 100+ unique activities • Supports 4,000+ cloud app connectors for SaaS and IaaS	• Limited App Coverage & Allow/Block only except for complex MIME-Type • Regex matching for up/download
Dynamic detection of application instances and users in managed and unmanaged cloud apps independent of tenant restrictions	• Instance awareness for 500+ SaaS and IaaS apps including tenant discovery • Transparent, zero-config detection with robust controls	• No app instance awareness • Basic Tenant Restrictions / Few apps using header insertion
Data security engine with broad set of pre-defined compliance templates & data identifiers, full coverage of channels and comprehensive AI/ML	• Enterprise DLP with large set of AI/ML classifiers and train your own classifiers • Full data vector coverage across SaaS, IaaS, PaaS, web, email, endpoint	• Basic DLP prone to false positives/negatives • Covering Data-in-Motion for Web only, but no email/endpoint/SaaS/IaaS
Actionable user coaching for safe and productive business enablement of SaaS and GenAI apps	• Granular and contextual real-time user coaching enhancing user engagement and compliance with security guideline and fosters a security-first culture	• No concept of user coaching or education
Efficient Network and Security Operations		
Single management experience and policy framework for SaaS, public cloud, web, and private applications	• Netskope One Single Unified Console • Integrates with Netskope One SD-WAN functionality and policies	• Unified Console with limited capabilities
Single unified client across Secure Access Service Edge (SASE) infrastructures (including SSE and SD-WAN)	• Consistent deployment and operations to reduce attack surface and risk • Agentless available for unmanaged endpoints	• Single unified SSE client (“WARP” client) • No client support for SD-WAN
Digital Experience Management (DEM) to maximize network performance and user productivity with any device from anywhere to any app	• Netskope DEM combines Real User and Synthetic Monitoring, measures SSE platform processing time and provides proactive remediation via route control	• Limited DEM offering focused on synthetic tests via WARP client only
Advanced analytics with powerful visualization of controls effectiveness, risk factors, and remedial action recommendations	• Detailed visualization of user behavior and data flows • Connects effectiveness of controls to level of risk	• Limited reporting based on basic visualizations of simplistic metrics with no ability to go deep into risk or effectiveness of controls
Open platform offers deep integration into other security tools to improve overall value in reducing risk, improving business agility, and cutting costs	• Netskope Cloud Exchange offers 90+ deep integrations with third parties • Contributes context for Zero Trust Engine and telemetry for IR and SOC	• Limited 3rd party deep integration, mostly handing off traffic to the 3rd party for processing and/or visualization