High Impact Differentiators (Updated 2025-09-29)	Netskope	Microsoft
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	● Entra SSE is Azure based with only ~40 full compute regions ● Gartner does not list MS in SSE MQ due to lack of threat and endpoint support
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	● Current network infrastructure is not built for single pass optimization ● No SSL inspection capabilities (beta) and no inline threat or data inspection
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	● Extremely limited localization and geo-fencing rulesets with costly subscription ● No support for Dedicated egress IP or Localization Zones
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	● Global private network is resilient but not proven for inline inspection ● Unproven performance and latency when connected to MS Graph at scale
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	● Large gaps in real-time inline inspection common without private network use ● Legacy identity-centric architecture limits visibility and control over user traffic
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	● Microsoft Entra SSE focuses on M365 with limited scope for non-MSFT apps ● Primary focus on email security with MS 365 while ignoring other larger vectors
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	● Supports deception threat detection and limited UEBA for inbound user actions ● No comparable capability to score or action app risk with granular policies
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	● Very limited SWG capabilities (e.g. no SSL inspect, no URL recat, no RBI) ● Lacks inline reverse proxy CASB capabilities for unmanaged device access
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 ability to provide deep instance visibility or control ● Very limited support of tenant restrictions across a small set of SaaS apps
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	● No holistic data protection beyond basic DLP with limited web, SaaS, IaaS ● Fragmented DLP engines and policy management across products
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 effective user coaching - using “connection reset” browser error for HTTPS ● Blocking only with no opportunity for end users to justify activity
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	● Multiple Consoles (Entra SSE, many “Defender” consoles, Sentinel) ● Separate vendors and consoles for SD-WAN
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	● No SD-WAN capabilities for branches or clients ● Relying on SASE partnerships with separate consoles/vendor contracts
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	● Poorly-integrated SSE capabilities create challenges for root cause analysis
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	● High level overview analytics mostly focused on device/endpoint security ● Limited reporting (~20 reports)
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 contextual correlation between product lines