High Impact Differentiators (Updated 2024-12-09)	Netskope	Skyhigh Security
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 76+ unique true-compute metro regions for globally-optimized, interconnected, and resilient connectivity	• Only ~40 Metro Regions with true compute for Cloud SWG plus Skyhigh ZTNA and CASB in some regions creating inferior and unpredictable experience
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	• Hidden backhauling due to use of vPOPs in majority of listed locations • No single pass due to missing platform integration
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	• Some regions offer only a subset of services (e.g. SWG only, ZTNA only) • Limited Localization Zones through 50+ vPOPs and no DEIP support
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	• 99.999% uptime SLA for cloud web and 99.5% for CASB. • Latency SLA based on average delays that hides issues with traffic spikes
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 (activity, instance, user risk)
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	• Most real-world deployments are bypassing O365 from steering/SSL-inspect • Limited visibility & controls and no instance awareness
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	• Tens of thousands of fewer apps with only a few weaker criteria • Limited “check the box” UEBA anomaly detectors
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	• Basic activity controls for far fewer apps • Claim support for “any” app but limited controls apply
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	• Basic allow/block tenant restrictions with no application instance awareness • No discovery workflow for non-corporate tenants
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	• Cloud-Native DLP misses advanced DLP methods like OCR and ML-based • Requires Trellix ePO console with totally different design language and logic
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	• Limited coaching based for browser-access, but not native app
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	• Claims single console but complete offering requires at minimum 3 different consoles and on-premises management
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 • Requires separate SD-WAN vendor integrations
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	• No DEM capabilities except for basic transaction timing in event logs • 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	• 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 to bi-lateral exchange with limited IOC exchange • Technical alliance partnerships and integrations limited to IDP/SIEM/SD-WAN