| High Impact Differentiators (Updated 2025-09-29) | Netskope | Zscaler |
|---|---|---|
| **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 | ● ~43 Unique Metro Regions with varying services + 20 regions with surcharge<br>● Only partial peering to major CSPs; mix of private / public clouds and vPOPs |
| 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<br>● Single pass Zero Trust Engine with no backhauling to deliver security controls | ● Hidden backhauling due to use of vPOPs in various locations<br>● Conditional Access IP-based policy require ZIA to ZPA connector backhauling |
| 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<br>● Localization Zones for 200+ countries & Dedicated Egress IP in every region | ● Some regions offer only a subset of services (e.g. ZPA only)<br>● Limited Localization Zones & Dedicated IPs with cumbersome backhauling |
| 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<br>● 99.999% uptime with latency SLA based on 95th percentile | ● Commits to 100ms SLA for all traffic (2-10x worse)<br>● 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 assessment due to lack of contextual awareness of the application and application instance being used or the user activity being performed |
| **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<br>● Addresses the most significant risk, attack surface, and data exfiltration vector | ● Most real-world deployments are bypassing M365 from steering/SSL-inspect<br>● 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<br>● Advanced UEBA with 125+ ML models to identify insider threats | ● Covers less than half of Netskope discovered apps - blind to 50% of all apps<br>● Very basic “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<br>● Supports 4,000+ cloud app connectors for SaaS and IaaS | ● Basic activity controls, such as upload, post, send, etc., for far fewer apps<br>● No granular decoding of activities leading to mostly allow/block approach |
| 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<br>● Transparent, zero-config detection with robust controls | ● Basic allow/block tenant restrictions and Instance awareness for very few apps<br>● No ability to discover SaaS tenants already in use for most 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<br>● Full data vector coverage across SaaS, IaaS, PaaS, web, email, endpoint | ● Basic DLP which lacks compliance templates, contextual awareness and depth (e.g. limited file types) with weak AI/ML support and no trainable classifiers |
| 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 without support for a justify/proceed workflow<br>● No notifications in many deployments without client connector |
| **Efficient Network and Security Operations** | | |
| Single management experience and policy framework for SaaS, public cloud, web, and private applications | ● Netskope One Single Unified console<br>● Integrates with Netskope One SD-WAN functionality and policies | ● Partially unified consoles (ZIA/ZPA/ZDX), but still many separate consoles for Incident and posture management, connectivity and overall risk 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<br>● Agentless available for unmanaged endpoints | ● No SD-WAN client capabilities or true SD-WAN solution<br>● Branch/Cloud connector lacks SD-WAN capabilities |
| 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 | ● Relying on synthetic probes only measuring front door of an application<br>● No measurement of the SSE platform processing time |
| Advanced analytics with powerful visualization of controls effectiveness, risk factors, and remedial action recommendations | ● Detailed visualization of user behavior and data flows<br>● 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<br>● Contributes context for Zero Trust Engine and telemetry for IR and SOC | ● Limited to bi-lateral exchange with limited IOC exchange<br>● Charging separately for cloud-to-cloud log streaming |