

High Impact Differentiators	Updated 2025-09-29	Netskope	Cato Networks
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		<ul style="list-style-type: none"> • Dedicated NewEdge private security network spans 78+ unique true-compute metro regions for globally-optimized, interconnected, and resilient connectivity 	<ul style="list-style-type: none"> • Offers ~80 true unique metro regions and focuses on globally-optimized interconnectivity and resilience. Not recognized by Gartner SSE MQ, though.
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		<ul style="list-style-type: none"> • No added latency due to third-party cloud provider path inefficiencies • Single pass Zero Trust Engine with no backhauling to deliver security controls 	<ul style="list-style-type: none"> • Support Single Pass Multi Inspection for only limited set of capabilities • Supports "Smart Egress" for dynamic steering and egress control
Every user connection to global private network offers in-country localized experience, access to geo-fenced content and source IP restricted apps		<ul style="list-style-type: none"> • All metro regions offer all services to all customers • Localization Zones for 200+ countries & Dedicated Egress IP in every region 	<ul style="list-style-type: none"> • Dedicated Egress IPs are supported for select data centers only • Limited Localization Zones for ~40 regions where Cato has no footprint
End users experience low latency and high availability with all traffic steered through global private network		<ul style="list-style-type: none"> • Commits to 10ms SLA for non-decrypted and 50ms SLA for decrypted traffic • 99.999% uptime with latency SLA based on 95th percentile 	<ul style="list-style-type: none"> • 99.999% availability, but with a poor service credit, e.g. 5% credit for 98%. • No processing latency SLA
Deep real-time visibility into and control over user risk and trustworthiness during user sessions		<ul style="list-style-type: none"> • Continuous Adaptive Trust processed in real time for user, application, device, and data risk signals, including user behavior and application instance 	<ul style="list-style-type: none"> • Limited risk evaluation due to lack of contextual awareness and lack of app risk, activity risk, instance risk, 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)		<ul style="list-style-type: none"> • Full SSL decryption and inspection of all SaaS traffic including M365 • Addresses the most significant risk, attack surface, and data exfiltration vector 	<ul style="list-style-type: none"> • Recommends bypassing of significant traffic, including MS 365 • 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		<ul style="list-style-type: none"> • 80,000+ apps with ~60 risk criteria across key domains to improve TPRM • Advanced UEBA with 125+ ML models to identify insider threats 	<ul style="list-style-type: none"> • Extremely limited cloud apps catalog without deep risk analysis • Limited CASB-API and no UEBA or SaaS Security Posture Management
Real-time control of cloud applications using predefined activities across thousands of applications and millions of websites		<ul style="list-style-type: none"> • Patented Zero Trust Engine which decodes 100+ unique activities • Supports 4,000+ cloud app connectors for SaaS and IaaS 	<ul style="list-style-type: none"> • Primitive activity controls focused on few social media and file sharing apps • Extremely limited number of apps supported without deep risk analysis
Dynamic detection of application instances and users in managed and unmanaged cloud apps independent of tenant restrictions		<ul style="list-style-type: none"> • Instance awareness for 500+ SaaS and IaaS apps including tenant discovery • Transparent, zero-config detection with robust controls 	<ul style="list-style-type: none"> • Basic allow/block tenant restriction & limited application instance awareness • No understanding of risk associated with 3rd party tenants
Data security engine with broad set of pre-defined compliance templates & data identifiers, full coverage of channels and comprehensive AI/ML		<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Basic DLP, lacking contextual awareness, depth or expertise • Initial unproven EDM/OCR/ML support and no coverage for email or endpoint
Actionable user coaching for safe and productive business enablement of SaaS and GenAI apps		<ul style="list-style-type: none"> • Granular and contextual real-time user coaching enhancing user engagement and compliance with security guideline and fosters a security-first culture 	<ul style="list-style-type: none"> • 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		<ul style="list-style-type: none"> • Netskope One Single Unified Console • Integrates with Netskope One SD-WAN functionality and policies 	<ul style="list-style-type: none"> • Single unified SASE console • Lacking core SSE capabilities like SSPM, DSPM, UEBA or in-house RBI
Single unified client across Secure Access Service Edge (SASE) infrastructures (including SSE and SD-WAN)		<ul style="list-style-type: none"> • Consistent deployment and operations to reduce attack surface and risk • Agentless available for unmanaged endpoints 	<ul style="list-style-type: none"> • In-house SD-WAN offerings fully integrated • No SD-WAN client capabilities or mobile/cellular gateways for micro-branches
Digital Experience Management (DEM) to maximize network performance and user productivity with any device from anywhere to any app		<ul style="list-style-type: none"> • Netskope DEM combines Real User and Synthetic Monitoring, measures SSE platform processing time and provides proactive remediation via route control 	<ul style="list-style-type: none"> • Basic DEM capabilities limited to latency measurement • Offers managed ISP monitoring services for mid-market
Advanced analytics with powerful visualization of controls effectiveness, risk factors, and remedial action recommendations		<ul style="list-style-type: none"> • Detailed visualization of user behavior and data flows • Connects effectiveness of controls to level of risk 	<ul style="list-style-type: none"> • Relies on 3rd party SIEM to which logs are streamed to • Lacks deep visibility into cloud activity, instances, risk, control effectiveness
Open platform offers deep integration into other security tools to improve overall value in reducing risk, improving business agility, and cutting costs		<ul style="list-style-type: none"> • Netskope Cloud Exchange offers 90+ deep integrations with third parties • Contributes context for Zero Trust Engine and telemetry for IR and SOC 	<ul style="list-style-type: none"> • Limited concept of risk (app, user, data) prevents any meaningful contextual correlation of risk with 3rd parties. Some SIEM/IDP integrations.
<small>Disclaimer - All content in this document may not be republished or shared with any third parties. All information provided is for informational purposes only. It is not a substitute for your own actual product testing and verification. While the information in this document has been verified using public information, no guarantee is implied that information may not have changed or is free of errors.</small>			