High Impact Differentiators (Updated 2025-10-13)	Netskope	Palo Alto 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	• Dedicated NewEdge private security network spans 78+ unique true-compute metro regions for globally-optimized, interconnected, and resilient connectivity	• Public cloud based (GCP/AWS/OCI) with only ~45 full compute regions • Multiple surcharges for additional access locations, service connections, etc.
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 “front doors” in various locations • Advanced Threat and DLP inspection require service-chaining to fewer POPs
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	• Many regions offer subset of services (e.g. DLP in very few regions) • Limited Localization Zones & Complex, non-contiguous Dedicated Egress IPs
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	• Commits to vague one-way “packet processing” SLA, not round-trip time • Limited full compute leads to back-hauling and latency for advanced services
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 • Addresses the most significant risk, attack surface, and data exfiltration vector	• Most real-world deployments are bypassing M365 from steering/SSL-inspect • 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	• SaaS app have weaker evaluation criteria/control • Very basic UEBA anomaly detectors not capable of surfacing insider risk
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, such as upload, post, send, etc., for far fewer apps • 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 • Transparent, zero-config detection with robust controls	• Basic allow/block tenant restrictions and Instance awareness for very few apps • No ability to discover SaaS tenants already in use
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 which lacks compliance templates, contextual awareness and depth (e.g. limited file types) with weak AI/ML support and limited 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	• Bad User Experience: No notifications leaving user in the dark • Lack of user-centric workflows to coach, warn or redirect users
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	• Requires costly Strata Cloud Manager Pro add-on for single console mgmt • Legacy Panorama customers must continue to use Panorama, not SCM
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	• In-house SD-WAN offerings partially integrated • No unified SD-WAN client
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 • 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 • 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 • Charging separately for Cortex Cloud Log Storage

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.