



Netskope Zero Trust Engine

Thank you for downloading this Netskope solution brief. Carahsoft is the reseller for Netskope FED and SLED solutions available via GSA 2GIT, CMAS, GSA MAS, and other contract vehicles.

To learn how to take the next step toward acquiring Netskope's solutions, please check out the following resources and information:



For additional resources:
carah.io/Netskope-Resources



For upcoming events:
carah.io/Netskope-Webinars



For additional BlackBerry solutions:
carah.io/Netskope-Solutions



For additional FED and SLED solutions:
carah.io/Netskope-Solutions



To set up a meeting:
netskope@carahsoft.com
(833) 478-1740



To purchase, check out the contract vehicles available for procurement:
carah.io/Netskope-Contracts

Netskope Zero Trust Engine

Accelerate your zero trust initiative and secure hybrid work with Netskope One and the Netskope Zero Trust Engine. Delivering unmatched contextual awareness, Netskope enables you to build adaptive, precise, multi-layered policies based on zero trust principles. Establish least-privileged access across users, applications, and data to stop any modern threat and all without users having to think differently.

Quick Glance

- **Precise:** Unparalleled context awareness that leads to the most precise adaptive trust policies, minimizing risk exposure to the organization.
- **Fast:** Processes traffic at the speed of business, connecting users to the web, cloud, or private apps, securing transactions with no user experience trade-off.
- **Comprehensive:** Part of a complete, integrated platform that offers extensive threat and data protection across web, cloud, and private applications.

The Challenge

As exposure to cybersecurity risks continues to peak, it has become increasingly vital for organizations to have visibility of their unique risk landscape and have a response strategy that can be deployed at scale across any application and environment.

While adopting a zero trust approach has been the answer for quite a while now, the expanding scope of modern enterprise has made it very hard for organizations to lock down data wherever it exists and adopt a zero trust strategy without slowing down business productivity and performance.

The transitioning of applications and workloads to the cloud, adoption of hybrid work models, and explosion of data beyond the data center to devices, apps, networks, and clouds have left organizations grappling with the right zero trust focused security approach.

Netskope Zero Trust Engine

The Zero Trust Engine is at the heart of the Netskope One platform, facilitating your implementation of zero trust and policy rules by continuously gathering risk telemetry about users, devices, applications, and data. This telemetry drives a unified, precise and comprehensive adaptive trust policy that minimizes security risk while enabling a positive user experience.

Netskope's Zero Trust Engine delivers continual adaptive trust across three levels:

- Risk context **awareness** across identity, application, user behavior, device, and cloud
- Precise, powerful policy **definition**
- Flexible, empowering multi-layer policy **enforcement**

Enhanced visibility with precise context and multi-layered policy enforcement

Implementing zero trust principles like least-privileged access demands enhanced visibility across a number of contextual variables, including application instance, user activity, data sensitivity, and more. This awareness of context needs to further translate into a granular policy that reflects nuance and can be deployed at scale.

The Netskope Zero Trust Engine features unparalleled context awareness that leads to the most precise adaptive trust policies, minimizing risk exposure. Key capabilities that make the Zero Trust Engine the most precise include:

- **In-depth contextual visibility across users, devices, data, and applications** to develop a complete, granular risk profile of every transaction in real time, including Netskope's unique "Layer 8" visibility that provides insight into crucial 50+ variables including:
 - Instance awareness—Is the user accessing a corporate or personal account?
 - Action awareness—What action is being performed? A share? Edit? Upload?
 - Behavioral anomalies—Is this an action normally performed? Are there unusual aspects to the access location or time? Are the number of action requests higher than normal?
 - Application trust—One of the largest repositories in the industry with over 75,000 applications.
- Incorporates even the most fine-tuned contextual factors to enable the **creation of adaptive trust policies that fully deliver the most precise least-privileged access.**
- AI/ML-based policies that automatically adapt to changing business requirements as applications evolve, new ones arrive, and old ones are decommissioned.

Netskope offers unparalleled contextual awareness for the most precise and granular real-time adaptive trust policies.

Netskope's Zero Trust Engine leverages its single-pass architecture to inspect any type of traffic in an average of <15 ms!

High performance with zero trust focused security

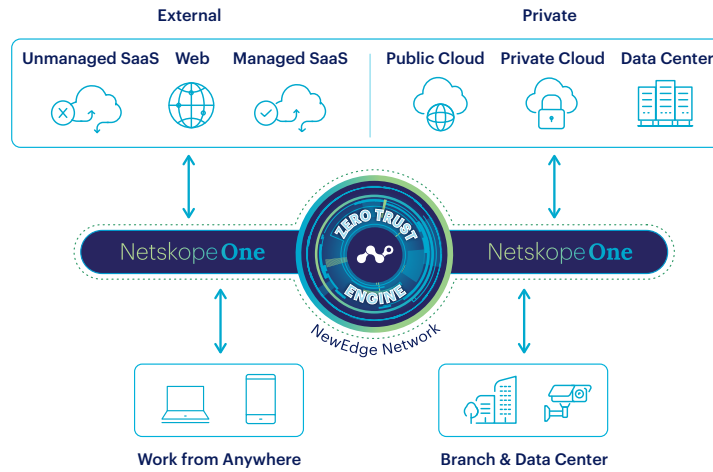
Zero trust inspection shouldn't cause friction: For every transaction, traffic needs to quickly get into the engine, be decrypted and decoded, and then scanned by a number of controls to assess and mitigate risk, all before it moves on to the destination. If traffic inspection negatively impacts performance, users will be encouraged to find ways to circumvent security controls.

The Netskope Zero Trust Engine processes traffic in milliseconds, actioning a security policy to the web, cloud, or private apps faster than any other vendor. Characteristics that make the Zero Trust Engine the fastest include:

- [NewEdge](#), Netskope's purpose-built network and private cloud infrastructure, features ultra-fast on-ramps for users and offices to connect to the Zero Trust Engine, as well as extensive peering relationships with the world's leading web and cloud providers to ensure **best-in-class, end-to-end latency.**
- Ability to decrypt and re-encrypt huge volumes of SSL traffic, and fully decode API and JSON—the language of the cloud—in milliseconds. Unlike some solutions that only decrypt or decode some traffic and exclude critical SaaS apps, the Zero Trust Engine provides **real-time decryption and decoding of all applications and sites** without impacting user experience.
- An **elegant single-pass architecture that performs an array of security inspections in real time.** In contrast to other security solutions with fragmented security controls, the Zero Trust Engine ensures that in-depth security inspection doesn't come at the cost of latency.

The performance of the Zero Trust Engine is backed by industry-leading SLAs, processing decrypted transactions in <50 ms and non-decrypted transactions in <10 ms.

Netskope One



Reduce complexity and fragmentation with comprehensive security

Adopting zero trust principles isn't just about granular access controls. It is about extending an array of security capabilities to fully inspect transactions continuously based on context to preserve trust. Any security solution that is lacking in vital security controls or not able to deliver security consistently across all traffic types will undermine an organization's security posture and zero trust initiatives.

Netskope's Zero Trust Engine is part of a complete integrated platform that offers comprehensive threat and data protection across web, cloud, and private applications. Characteristics that make the Zero Trust Engine the most comprehensive include:

- The Zero Trust Engine **is at the center of Netskope's converged network and security platform**, which ensures that zero trust policy extends effortlessly and consistently across Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), Cloud Firewall (FWaaS), and Software-Defined WAN (SD-WAN) services, leaving no security gaps.
- **Best-in-class threat and data protection** featuring an extensive range of features, bolstered by cutting-edge AI and ML capabilities, that lead the industry in terms of efficacy. Many competing solutions provide under-featured threat protection suites, and others lack any sophisticated data protection capabilities, despite the data-centric nature of zero trust.
- **Tight integration with ecosystem partners, including leading XDR and IAM vendors**, to help deliver complete zero trust architectures that exceed what any single vendor solution can deliver in terms of completeness.

Secure and harmonious user experience

Restricting users with broad, rigid security policies hampers user productivity and can ultimately increase security risk because users will always find a way to circumvent these measures. Netskope's Zero Trust Engine empowers users by allowing permitted interaction with applications augmented with "in the moment" coaching and user feedback, enabling them to take a role in the organization's security. Moreover, with real-time user coaching built into the Netskope One Client, the user experience is seamless and consistent.

Characteristics that make the Zero Trust Engine the most comprehensive policy engine include:

- Security enhancement options like step-up authentication or Remote Browser Isolation (RBI) add an extra layer of security that allows users to access resources with higher risk profiles.
- Users are involved in the security process with **AI-driven user coaching that guides them toward making better security decisions**. This results in better user experience when compared to simply denying access.
- Continuous inspection and verification of user behavior to identify deviations from baselines and thereby detect malicious insiders, compromised accounts, data exfiltration and brute-force attacks.

To adopt the right zero trust approach, it is vital for organizations to first and foremost understand where they are in their zero trust journey and where they want to be.

BENEFITS	DESCRIPTION
Reduce administrative complexity with an integrated platform	The Zero Trust Engine powers the Netskope One platform, consolidating network and security solutions to lower costs and delivering a single console and policy framework for greater operational efficiency.
Enable advanced investigations	With all types of traffic—apps, cloud services, and web—being decoded by the Zero Trust Engine, an organization can collect rich metadata for analytics and increase visibility for investigations and incident response.
Enable seamless user experience with on-demand Isolation	Target and Extended Remote Browser Isolation (RBI) to ensure browsing on risky or unsanctioned web categories is isolated contextually and user productivity is not hampered.
Remove implicit trust with adaptive access	Trigger granular controls based on deep understanding of context and content across all inspected web and cloud traffic.
Maintain a strong security and trust posture	Comprehensive real-time risk assessment and trust scoring with unequaled breadth (75k+ apps) and depth (50+ attributes).
Reduce risk with continuous threat and data protection	Industry-leading threat and data protection across web, cloud, and private apps to reduce risk of breaches or data loss incidents.
Consistent policy enforcement across all channels	Powerful, precise, converged policy across web, cloud, and private apps.



Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit [netskope.com](https://www.netskope.com).

©2024 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 02/24 SB-720-1