netskope

WHITE PAPER

Federal Transformation with SASE-based TIC 3.0 Solutions

Zero-trust access with cloud-native advanced data and threat protection for cloud and web

INTRODUCTION

The Trusted Internet Connection (TIC) version 3.0 advances to a cloud-first perspective providing federal teams the opportunity to leverage cloud and mobility. While zero-trust network access (ZTNA) can replace legacy VPNs for direct access to private apps and resources in public cloud or private data centers, it requires pairing with cloud-native secure access service edge (SASE) networking and defenses. The difference from legacy web solutions that are cloud hosted—or in the cloud—from defenses designed to decode cloud traffic—or for the cloud—becomes very apparent when analyzing capabilities. At the core of SASE defenses is data context of cloud communications for granular policy controls, plus advanced data and threat protection.

Why TIC 3.0?

The modernization to version 3.0 of TIC expands upon the original program to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications.

Originally established in 2007, TIC is a federal cybersecurity initiative intended to enhance network and perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative, setting requirements and an execution framework for agencies to implement a baseline perimeter or multi-boundary security standard.

TIC 3.0 Security Capabilities

The security capabilities listed in the TIC 3.0 Security Capabilities Catalog define the protections foundational to the TIC initiative and provide protections for information being processed, stored, or transmitted by information systems. The Security Capabilities Catalog guides agencies to apply risk management principles and best practices to protect federal information in various computing scenarios within the TIC 3.0 Reference Architecture and use cases. Security capabilities within TIC 3.0 are applied by policy enforcement points (PEPs) consisting of security devices, tools, services, or applications enforcing the security capabilities. The general concept suggests PEPs can be placed along the path of data flowing between client and server, and optimized by location for effectiveness as shown in Figure 1 below.

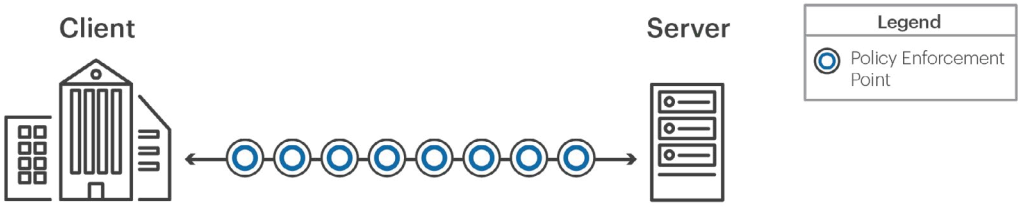


Figure 1: *Security capabilities placed along data flows*

This is augmeted by the concept of trust, shown by various colors along the data flow based on PEP security capabilities as shown in Figure 2. Modern cloud defenses also provide confidence scoring for cloud applications and services, plus a user confidence index, both providing scoring beyond the data path trust level itself. This enables granular policy controls based on user confidence, app/server confidence, data classification, and the data path, locations, and devices utilized.

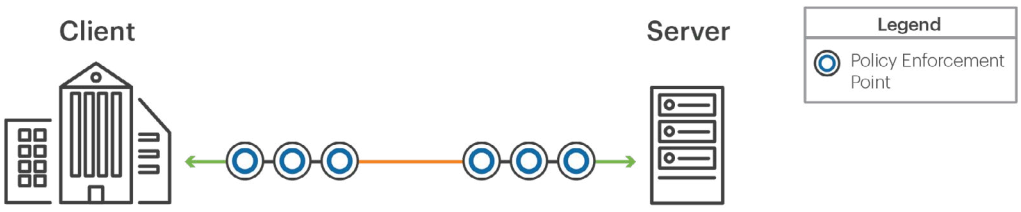


Figure 2: *Security capabilities of PEPs impact the degree of trust*

Multiple PEPs can also be grouped together for efficiency and as a demarcation point for data flows as shown in Figure 3 below. Leading analyst firms such as Gartner have defined this concept as secure access service edge (SASE) architecture where security and networking services are combined and provided as a 'heavy cloud edge' close to users. Data context is a core principle of SASE architecture found in newer defenses able to decode app and cloud service content, along with an understanding of activity, app instance, and other variables to provide context for granular policy controls.

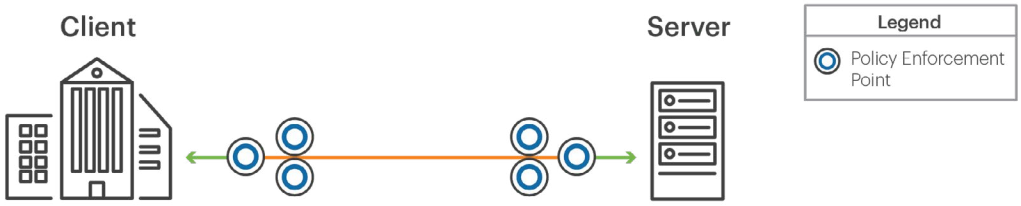


Figure 3: *Grouping PEP security capabilities together in shared positions*

As users, apps, and data migrate to the cloud, the traditional perimeter inverts to a cloud security edge with multiple security capabilities invoked by a forward proxy to inspect encrypted TLS traffic for data context, threats, and data theft. For managed devices, endpoint controls remain while unmanaged devices from other agencies or the public can be addressed by reverse proxy inspection from the cloud security edge for managed cloud apps.

While PEPs are focused on data flows in TIC 3.0, requests for understanding user behavior anomalies and user confidence index ratings are increasing alongside the existing capability to provide app and cloud service confidence ratings. Understanding data movement, including unintentional and unapproved data activity is a top use case often paired with the objective of using real-time coaching to improve user actions and behavior.

Trust Zones and Levels

A trust zone noted by a circle in the reference architecture is a discrete computing environment involved in information processing, storage, and/or transmission that share the same applicable security capabilities necessary to protect the zone. In Figure 4 the general concept is shown and mimics the concept of a traditional perimeter, however, trust zones can be divided by user, groups, networks, location, application, or browser level as examples shown in Figure 5. By extension, individual apps, cloud services, endpoints, and workloads may be considered as trust zones themselves, in line with zero trust principles. Solutions providing SASE architecture security capabilities often include zero-trust network access (ZTNA) security capabilities and are known to replace legacy VPNs in many use cases.

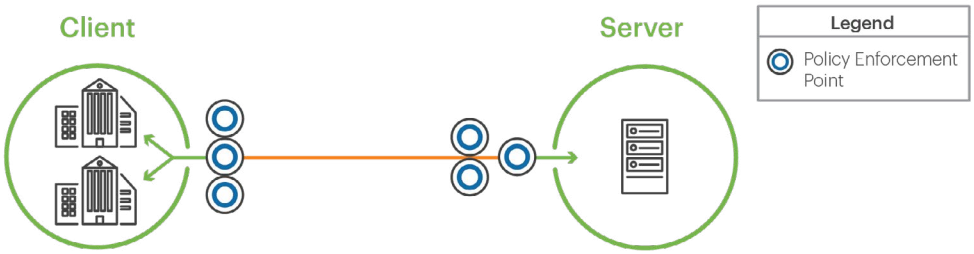


Figure 4: *Basic construct of trust zones with PEPs*

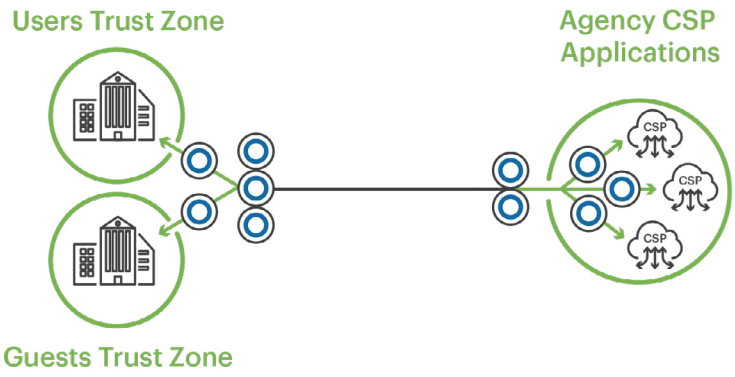


Figure 5: *Segmenting trust zones by user groups with PEPs*

The reference architecture provides three trust levels (e.g. high, medium, low) for trust zones as an example shown in Figure 6. An agency may have more trust levels depending on their security capabilities and environment. Examples within trust levels may include the degree of control, degree of transparency, and the ability for verification.

Figure 6: *Three tier trust level example with color coding*

Figure 7: *Trust level coarse grain examples*

Examples within the three tier trust levels are shown in Figure 7 and would best be described as coarse grained for an environment, location, or cloud service. Modern cloud defenses take this concept farther with confidence index ratings on users, apps, and provide advanced data protection including data classifications for exact data match, image and document classifiers, and fingerprinting with a degree of similarity as examples. This enables the trust zones to cover identity/user, apps, and data as primary security control planes for cloud security.

Management entities (MGMT) within the reference architecture include both organizations and products and/or services. These entities control the collection, processing, analysis, and display of information collected from the PEPs and allow administrators to control devices, access, data flows, and enable incident response. The combined metadata from multiple PEPs is valuable for investigations, queries, and threat hunting. Consolidation is one of the primary benefits of SASE architecture, plus less complexity and confusion as PEPs become cloud-based microservices within a single cloud platform and console.

Security Patterns and Use Cases

Security patterns describe end-to-end data flows between trust zones and may have an associated set of security capabilities. Figure 8 shows an example between an agency branch office and the web with a PEP in the data flow. Traditionally, the PEP would be an on-premises forward proxy web gateway appliance with URL filtering, content filtering, threat protection, and user/group access controls. Today, web gateways carry over half their sessions for cloud app traffic requiring a new set of capabilities including being cloud hosted for performance and scale, decoding app traffic for data context, and applying data and threat protection to cloud and web content.

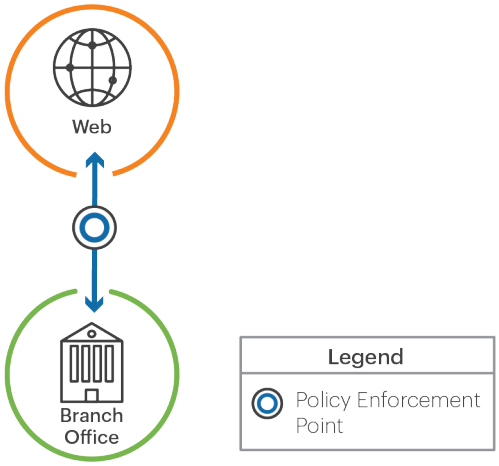


Figure 8: *Traditional agency branch office to web security pattern*

Agencies are encouraged to explore a variety of security patterns associated with TIC use cases beyond the examples provided. Specific to Figure 9, Option 1 follows the pattern of on-premises web gateway appliance defenses and the limitations may include performance issues and capacity limitations of hardware for TLS traffic inspection, defenses, storage, and peak loads.

Option 2 follows a traffic backhauling flow from the agency branch office through an agency campus where both locations may have on-premises defenses and has the added delay of reaching the desired web destination and then returning back to the user through the agency campus. Option 3 sends agency web traffic through a cloud-hosted CASB and gains the advantages of on-demand cloud performance and geographic scale for TLS traffic inspection, defenses, storage, and handling peak loads.

However, all three examples are limited to web traffic and lack the ability to decode and inspect cloud app communications and data context for data and threat protection.

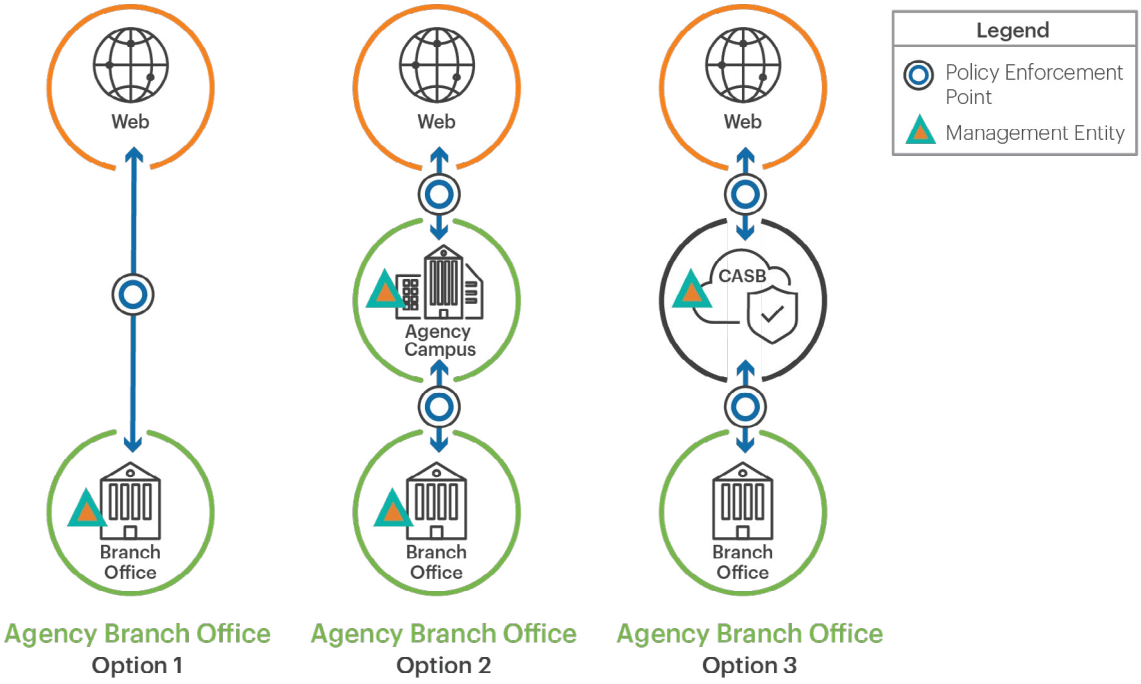


Figure 9: *Security pattern examples*

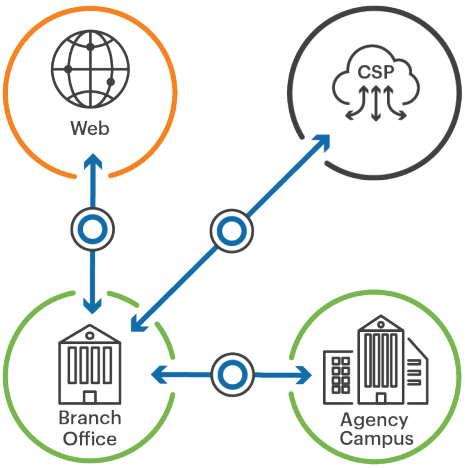


Figure 10: *Multiple security pattern example*

Use cases can be made up of multiple security patterns as shown in Figure 10. The agency branch office can directly access the web through a PEP, plus a CSP and an agency campus through additional PEPs. The value SASE architecture brings to this example is one solution covers all three PEPs in the diagram by providing secure web gateway (SWG), cloud access security broker (CASB), and zero trust network access (ZTNA) to private apps and resources.

A legacy approach would use SWG appliances, a cloud hosted CASB, and VPN concentrators between the branch office and agency campus. Using legacy VPNs brings the known issues of visibility, complexity, VPN concentrator issues, and a poor user experience, plus the liability of lateral movement within the external partner (or agency) via the VPN connection direction, and the risk of public exposure for the VPN connection service. The issues of legacy SWG appliances have already been reviewed.

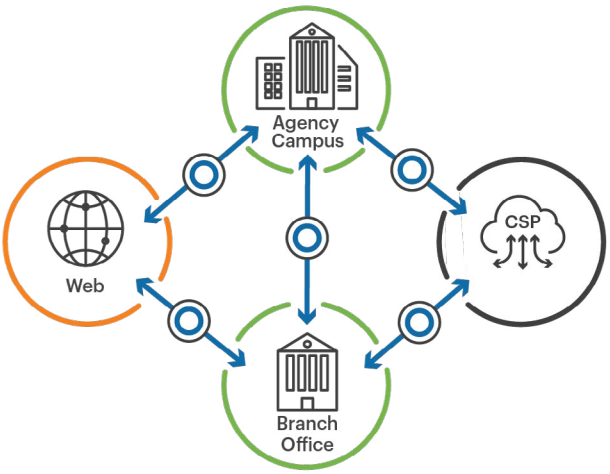


Figure 11: *Combining use cases example*

Combining multiple use cases takes the concept for TIC 3.0 to another level as shown in Figure 11. There are five PEPs in the diagram that could be implemented with three legacy solutions, or one SASE architected solution using a single platform, console, and shared policy controls to reduce complexity, configuration, administration, and even support remote users not shown in the diagram. While the diagram shows the web on the left and a CSP on the right, the reality is users are likely to visit the web, SaaS, IaaS/PaaS, custom apps, and private resources in their daily activities.

Evolving from the Traditional Perimeter

Digital transformation and increased remote working are inverting the traditional security stack perimeter known for its hard-shell perimeter and soft inside as shown in Figure 12. The path forward is users, apps, and data are outside the legacy perimeter on infrastructure out of your control and thus shifting security towards data protection and risk management. The commercial sector is well into this transformation journey as business units and users freely adopt apps by the thousands to enable the success of their companies. For agencies and departments, the process is beginning with TIC 3.0 use cases allowing for a more flexible perimeter definition and not backhauling traffic.

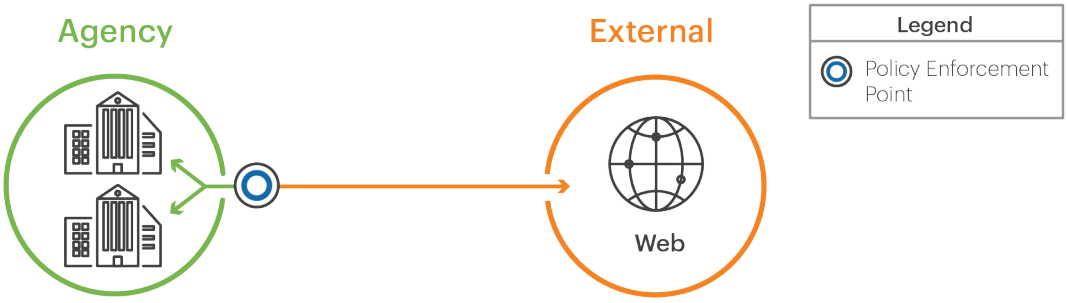


Figure 12: *Traditional perimeter example*

In Figure 13 an expanded example shows multiple trust zones and many PEPs to secure the agency in the center of the diagram. A legacy VPN could connect remote workers, branch offices, and partner agencies, however, the issues of lateral movement and exposure discussed earlier exist. The more likely path forward is zero trust network access to specific apps and resources. The green and red zone CSPs, plus web and public users could use legacy allow/deny controls by destination, however, these legacy defenses are missing the data context required for SASE architecture to enable data and threat protection of both web and cloud content, even if hosted 'in the cloud'.

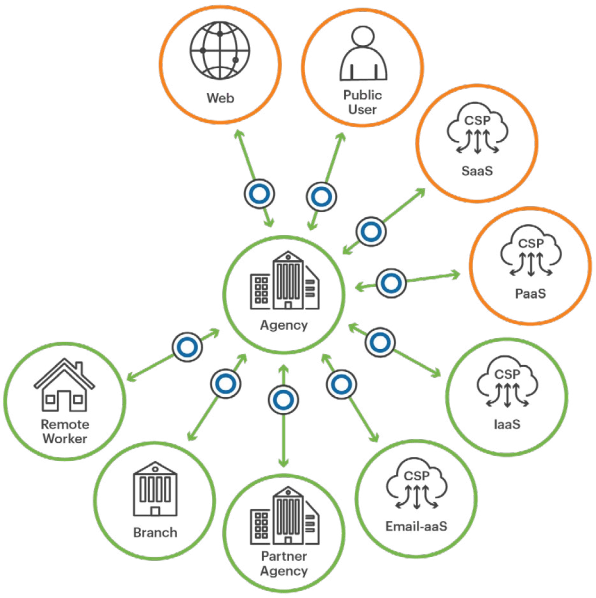
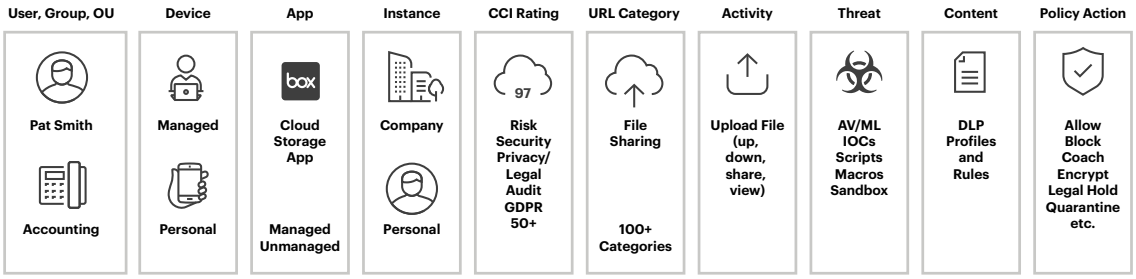


Figure 13: *Distributed agency trust zone diagram*

Where the difference in capabilities really surfaces is with 'for the cloud' defense capabilities by decoding and inspecting cloud (i.e. CSP) communications for thousands of approved CSPs to provide protection and to capture the data context of the traffic pattern flow alongside web communications. This is where the legacy capabilities of deep packet inspection (DPI) for allow/deny controls of web and cloud traffic show their limitations, unable to capture cloud native CSP data content and context by decoding the unique traffic of CSPs. Legacy web proxy solutions that can reassemble packets into sessions for web filtering also lack the ability to decode unique traffic to CSPs for data content and context. While these solutions can be 'in the cloud', they lack the 'for the cloud' capability to decode the cloud traffic of CSPs.

One of the primary principles of a single-pass cloud native SASE architected solution is data context. For any web or CSP desired destination can the data be analyzed with data and threat protection defenses? Even more so, for the instance or activity of the CSP as a frequent data exfiltration method is moving data between managed instances and personal instances of the same CSP, or between frequently accessed CSPs, or CSP categories. If a user can download data to their device, they can likely upload the data to a new location, and this makes Cloud DLP a critical capability for downloads and uploads to manage data risk for cloud and web communications. Whether intentional or accidental lack of context around instance awareness often leans to data exfiltration from managed CSPs. Below is an illustration for some of the granular policy controls providing data context from Netskope Cloud XD.



Pat from accounting - on desktop - using personal Box instance - uploading files - DLP check - coach if PCI, PII, etc.
Pat from accounting - on desktop - using company Box instance - uploading files - check for malware/threats
Pat from accounting - on mobile - using company Box instance - downloading files - view-only mode
Pat from accounting - on desktop - browsing web gambling site - block site - coach user with AUP alert

For an agency to benefit from digital transformation they will quickly find they need to allow more CSPs than they block, and this pushes basic allow/deny defenses out of the picture as what you allow needs granular policy controls for data context. Policy controls for trust zones can require step-up authentication, device classification and posture checks, and user confidence scores based on behavior analytics to drive pre-defined or on-demand policy actions.

Adding in Zero Trust Network Access

A single pass cloud native SASE solution should also provide zero trust network access as reviewed in the NIST Zero Trust Architecture SP 800-207 document, also described as private access in solution names. The green arrows in Figure 13 represent these communications where the user is provided access to only the requested resource (i.e. CSP, External Partner App, Agency Campus Internal App). A private access solution removes the risk of lateral movement within a destination, plus does not require any public exposure of services. Users benefit from a transparent private access experience to the apps and resources desired without the complexity and risks of a legacy VPN.

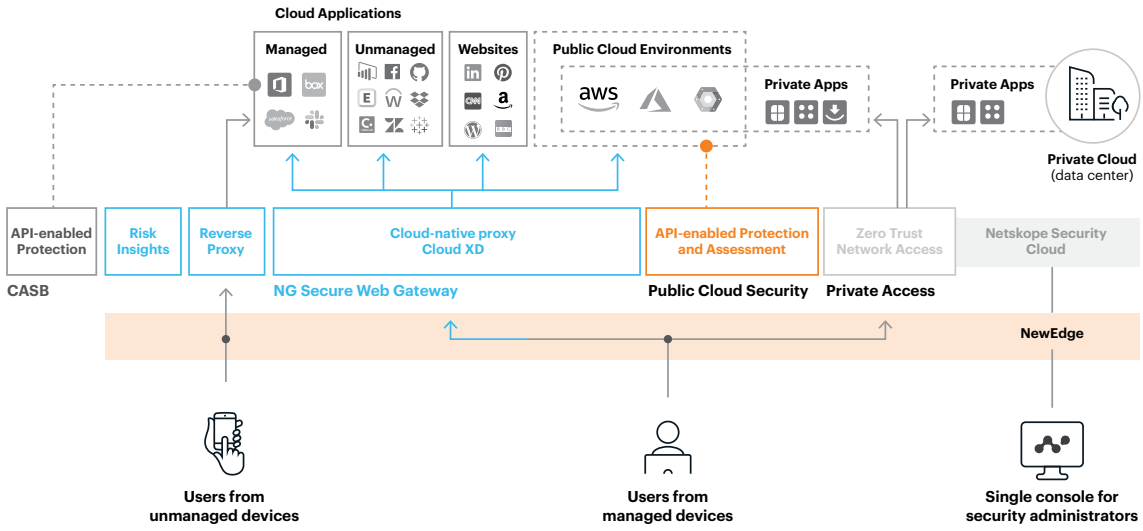
Netskope Provides an in the Cloud, and for the Cloud TIC 3.0 Solution

Netskope is FedRAMP authorized and has managed cloud-native inline proxy-based defenses for over eight years including Fortune 100 multinational customers. Unique to Netskope is our inline Cloud XD engine to decode thousands of cloud apps to apply rich granular policy controls with data context. For web and cloud communications Netskope provides unmatched Cloud DLP capabilities including machine-learning classifiers for documents and images, fingerprinting with degree of similarity, and exact data match capabilities.

Netskope Threat Labs focuses on web and cloud-enabled threats including cloud data risks. The unique visibility is leveraged for web and cloud traffic pattern capture and analysis, including machine learning threat detection, bare-metal sandboxing, behavior analytics, and developing new threat intelligence. Netskope leverages multiple threat intelligence feeds and enables bi-directional indicators of compromise (IoC) sharing with its Cloud Threat Exchange (CTE) for file hashes and malicious URLs with endpoint protection, SIEM, SOAR, IR, and other security stack solutions.

Netskope supports multiple TIC 3.0 security patterns and use cases with the visibility of Cloud XD for cloud and web communications, capturing use case traffic patterns with data context, and providing rich metadata and telemetry for sharing with CISA and DHS. This rich metadata also enables improved detection and machine learning, plus supporting investigations, response workflows, and threat hunting.

Netskope NewEdge provides multiple FedRAMP authorized data centers within the United States for access, data planes, management, and data storage. As a private network NewEdge is highly optimized for round trip times and is extensively peered with major cloud providers and supports TLS v1.3 secure communications. NewEdge avoids the congestion of the Internet, cost based routing preferences, and the limitations of public cloud providers for metro-city coverage of scalable virtual machine (VM) images. For example, you can run VMs in Ashburn, VA while in New York City your only option is bare-metal hardware with public cloud providers. NewEdge is designed as a secure and private network for large scale SASE solution architecture.



NETSKOPE SOLUTION CAPABILITIES

Next Generation Secure Web Gateway

Inline cloud and web proxy for HTTP and HTTPS traffic inspection using a steering client for web, SaaS, and IaaS/PaaS user traffic, and GRE or IPsec tunnels for offices.

Next Gen SWG includes the following capabilities:

Next Generation Secure Web Gateway

- Cloud native forward cloud and web proxy with SSO, MFA and AD integration
- Reverse proxy for managed cloud services and apps with IdP integration
- TLS traffic inspection including v1.3 natively with cloud performance and scale
- Cloud XD decodes thousands of managed and unmanaged cloud services and apps
- Granular policy controls including app instance and activity awareness
- Cloud Confidence Index (CCI) risk ratings for thousands of cloud services and apps
- Analytics and reporting based on 90 days of data retention (longer by contract)
- Open REST API

Web Filtering

- URL filtering for 120+ categories, languages for 200+ countries, and 99.9% of the active web
- Filtering includes YouTube categories, translation services, SafeSearch, and silent ad blocking
- Dynamic web page categorization for 70 categories, plus site lookup tool and reclassification service
- Allow, block, or proceed with warning, plus custom alerts to system tray or web browser
- Create custom web filtering categories plus allow and deny lists
- Determine traffic inspection by URL category or domain

Advanced Threat Protection (ATP)

- Anti-malware engines, client traffic exploit protection, and true file type analysis
- 40+ threat intel feeds, plus import IOCs including malicious URLs and file hashes
- Cloud Threat Exchange (CTE) enables threat intel sharing with EPP, EDR, SIEM, etc.
- De-obfuscation and recursive file unpacking with support for 350+ families of installers, packers, and compressors
- Pre-execution analysis and heuristics for 3,500+ file format families, with 3,000+ static binary threat indicators for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types
- Bare-metal sandboxing for 30+ file types including executables, scripts, and MS Office documents for Windows operating systems with behavioral file analysis and the ability to defeat evasive techniques
- Machine learning deep analysis to detect unknown threats, anomalies, and behaviors
- UEBA sequential anomaly rules to detect bulk uploads, downloads, deletes, plus proximity, failed logins, rare events, risky countries, and data exfiltration between company and personal instances
- 3rd party sandbox and RBI integration

Behavior Analytics

- UEBA batch and stream machine learning (ML) analysis to detect insider threats, compromised accounts, and data exfiltration
- User confidence scoring and event correlation timelines with the ability to invoke policy actions based on score
- UEBA custom sequential anomaly rules with pre-defined templates

Advanced Data Protection (DLP)

- Data-in-motion DLP analysis for cloud services and apps, plus web traffic, files and forms
- 40+ regulatory compliance templates including GDPR, PII, PCI, PHI, source code, etc.
- Includes 3,000+ data identifiers for 1,400+ file types, plus custom regex, patterns, and dictionaries
- File fingerprinting with degree of similarity and exact data matching
- AI/ML classification for documents (patents, M&A documents, tax forms, source code), plus images (desktop screenshots, passports, IDs)
- Incident management and remediation

NewEdge Global Network

- Hyperscale, carrier grade global private network delivers the Netskope Security Platform from data centers around the world
- Fast performance for access to internet and cloud applications with minimal round-trip time
- Extensively peered with the major cloud providers

Netskope Private Access

Netskope Private Access (NPA) is a cloud based Zero Trust Network Access (ZTNA) solution that is a fully integrated component of the Netskope Security Cloud platform and delivered through the Netskope NewEdge network. NPA directly connects remote workers to private applications running in public cloud environments (i.e. CSPs) or private agency data centers; reducing risk and simplifying security operations.

NPA includes the following capabilities:

- Secure end-to-end connectivity using TLSv1.3 between remote users' devices and private applications
- Inline access policies that ensure that users are directly connected only to the applications they are authorized to use and do not have broad network-level access
- Support for browser-based access to web applications (e.g. HTTP or HTTPS applications) and for non-web / thick applications (e.g. SSH, RDP, Microsoft Windows Active Directory), plus support for both TCP and UDP protocols on almost all associated ports
- Integration with Microsoft Active Directory and Single Sign-On (SSO) providers to understand users, groups and organizational units, and therefore ensure only authorized users can gain access to applications
- Device security posture checking to ensure that only agency devices meeting a specific security posture can access agency or approved CSP private applications
- Use of the lightweight Netskope Client (supported on Microsoft Windows or Apple macOS devices) to steer application traffic to the Netskope Security Cloud using either DNS or the IP address

- Unlimited number of Netskope Private Access Publishers (supported on AWS, Azure, VMWare ESX, and any CentOS based virtual machine) to make private applications available to authorized users through the Netskope Security Cloud
- Network Events and Alerts for Private Application access retained for analytics and reporting for 90 days

Netskope CASB API-Protection

API-enabled cloud security for managed SaaS applications to monitor and control usage and protect data. Provides protection using APIs, granular policy enforcement, data and threat protection, analytics and reporting based on 90-day metadata retention.

CASB API Protection includes the following capabilities:

API-enabled Protection with visibility and granular policy controls for popular managed SaaS applications including:

- Microsoft Office 365 suite of apps, including Teams, Outlook, SharePoint, and OneDrive
- G Suite apps, including Gmail and Google Drive
- Slack Team and Slack Enterprise
- Salesforce
- Box
- Dropbox
- Cisco WebEx Teams
- Egnyte
- Github
- ServiceNOW
- Workplace by Facebook

Analytics and Reporting

- Analytics and reporting based on 90 days of data retention (longer, up to 1 year, by contract)
- Open REST API available for integration with third-party applications

Advanced Data Protection (DLP)

- Data-at-rest DLP analysis for managed cloud services and apps
- 40+ regulatory compliance templates including GDPR, PII, PCI, PHI, source code, etc.
- Includes 3,000+ data identifiers for 1,400+ file types, plus custom regex, patterns, and dictionaries
- File fingerprinting with degree of similarity, exact data matching and Optical Character Recognition (OCR)
- AI/ML classification for documents (patents, M&A documents, tax forms, source code), plus images (desktop screenshots, passports, IDs)
- Incident management and remediation

Advanced Threat Protection (ATP)

- Anti-malware engines and true file type analysis
- 40+ threat intel feeds, plus importing IOCs including malicious URLs and file hashes
- Cloud Threat Exchange (CTE) enables threat intel sharing with EPP, EDR, SIEM, etc.
- Unpacking and de-obfuscation, pre-execution analysis, and bare-metal sandboxing for 30+ file types
- UEBA sequential anomaly rules to detect bulk uploads, downloads, deletes, plus proximity,

failed logins, rare events, risky countries, and instance aware data exfiltration (between company and personal instances)
- Machine learning deep analysis to detect unknown threats, anomalies, and behaviors
- 3rd party sandbox integration

Netskope Public Cloud Security—Continuous Security Assessment

Continuous security assessment (CSA) is a Cloud Security Posture Management (CSPM) solution for AWS, Azure and GCP via API deployment to help organizations align their configurations to best practices and key compliance standards.

CSA includes the following capabilities:

- Continuously check for misconfigurations leading to potential exposures
- Supports top industry benchmarks and standards including CIS, PCI, NIST CSF, NIST 800-53, HIPAA/HiTrust, SOC2, ISO 27000, GDPR, CSA CCM, and Netskope Best Practices
- Detailed remediation guidance and response workflows

Netskope Public Cloud Security—IaaS Storage Scan

API-based security for Public Cloud (IaaS) Storage to scan and protect against data loss and malware. Support for AWS S3 Buckets and Azure Blob Containers.

Standard Data Protection (DLP) for IaaS includes compliance reports and templates, custom regex, patterns, dictionaries, AI/ML document classification, and incident management and remediation.

Standard Threat Protection for IaaS includes malware and threat detection, sandboxing executable files, threat intel feeds and IoC sharing.

ABOUT NETSKOPE FOR GOVERNMENT

Netskope enables government agencies and organizations to protect mission-critical data and personnel by securing usage of cloud managed and unmanaged applications (Shadow IT) and web access across all networks, locations, and devices, essentially the new perimeter.

At Netskope, we never stop delivering on the latest government requirements and needs, the toughest problems, and the best way to help our customers secure their mission in the cloud and on the web. TIC 3.0 helps to assure your compliance as we provide a full featured security stack built 'in the cloud', and 'for the cloud' where our customers can turn on the features they require when they need them.

Netskope's Security Cloud Platform meets the Federal Risk and Authorization Management Program (FedRAMP) requirements and has achieved FedRAMP Authorization.

For more information, please visit our website at netskope.com/solutions/government.

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey.

To learn more visit, https://www.netskope.com.