

SIFY MANAGED SASE OFFERING - NETSKOPE

PRODUCT DOCUMENT

May 2024



INTRODUCTION TO SASE



- **Secure Access Service Edge is a term defined by Gartner.**
- **Gartner introduced the concept of SASE in a research paper titled "The Future of Network Security Is in the Cloud," published in August 2019.**
- **SASE is a framework that combines network security functions with WAN capabilities.**

WHY SASE ?



WHAT

Application
Transformation

Network
Transformation

Security
Transformation

WHY



Support
increased
usage of cloud
applications
and services



Enhance
enterprise
agility and
operational
excellence



Improve overall
security
posture and
deliver better
user/app
experience

HOW



Cloud-Native
Security
Solution

(SASE)

SECURITY IS STRUGGLING TO KEEP UP



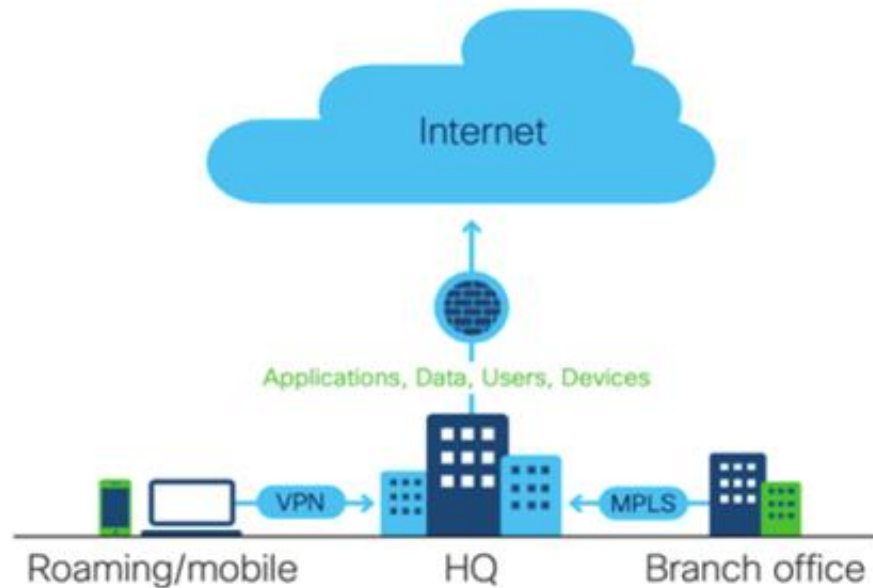
The hybrid workforce demands a faster, easier, more reliable **user experience**

Data sprawl across clouds & devices increases breach and compliance risk

Cloud-based **threats** evade traditional defenses, exposing enterprises to attacks

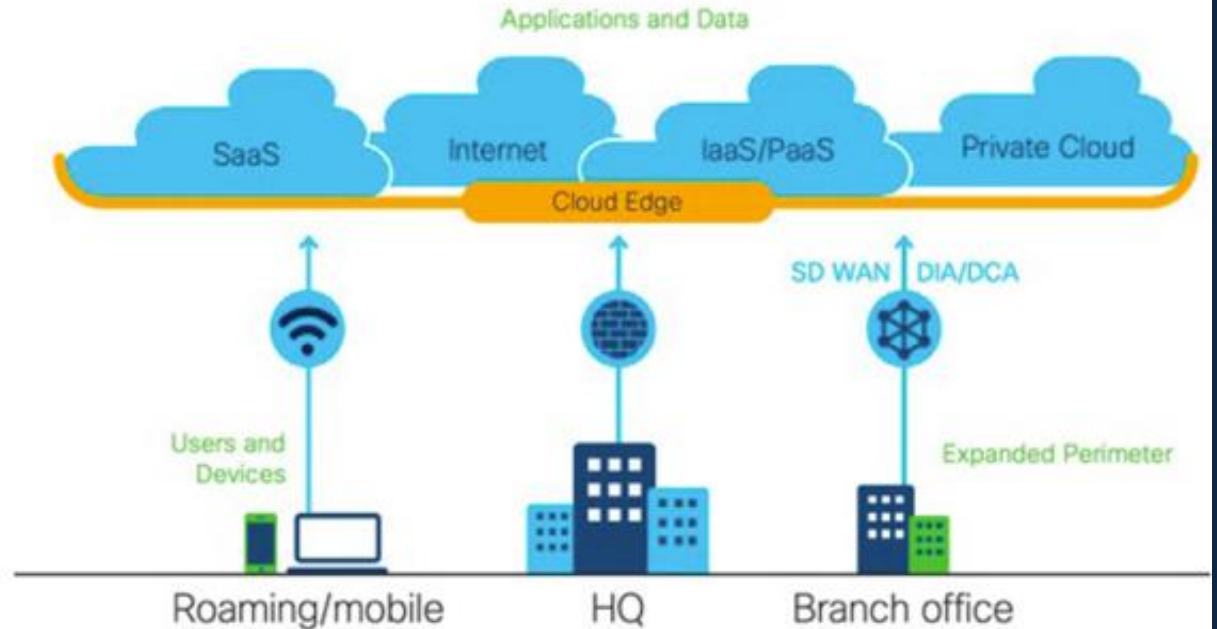
Disjointed security architectures drive up operating **cost & complexity**

CLOUD DRIVING MAJOR NETWORK ARCHITECTURE SHIFT



Legacy

Hub & Spoke Architecture with on-prem appliances



Today & Future

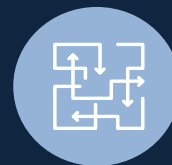
Leading Cloud Edge essential to delivering Networking & Security capabilities in the cloud



TOP CHALLENGES TO BE ADDRESSED



Balancing Hybrid
Work Dynamics



Expanding
Attack Surface



Generative AI's Complex
Landscape

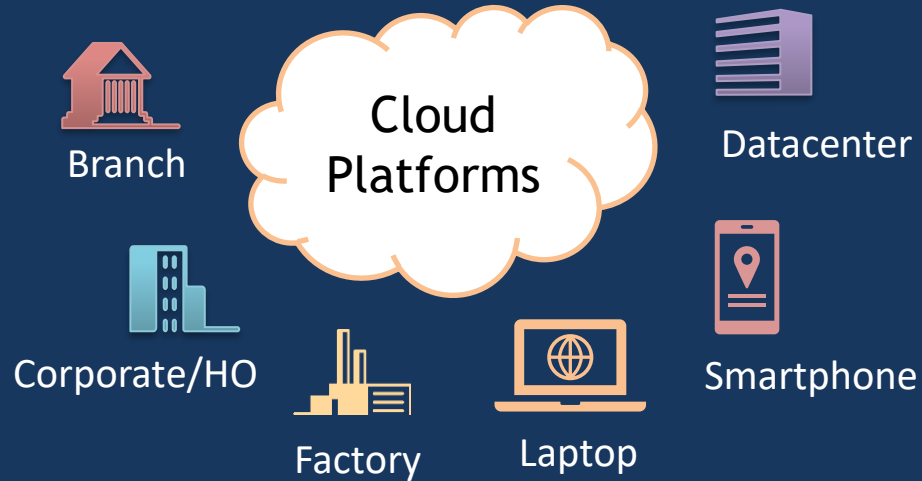


Threats within Trusted SaaS
Applications



Complexity of Data Privacy
and Regulations

SASE SERVICES



SASE helps Detect and Mitigate Threats, Connect and Secure Remote Workers, Identify and Protect Sensitive Data.

Security Service Edge (SSE) provides cloud-based, integrated security for secure access to websites, SaaS apps and private apps

Combines SD-WAN access and traffic monitoring functions in a unified solution for all types of accesses

Decreases Latency and enhance App and Network Performance by removing backhauled traffic flows

SASE Functionalities



- Secure Web gateway
- Firewall as a service
- Zero trust network access
- Cloud access security broker
- Remote Browser isolation
- Data loss prevention
- Network sandbox
- DNS Protection
- Web app & API Protection
- CDN, External DNS
- Legacy VPN
- Edge compute protection

Technology Partnerships :



BENEFITS OF SASE



Benefits	Description
• Flexibility	○ Offers direct access to cloud or network from any location to making simple implementation of novel digital business models
• Cost Savings	○ Security-as-a-service model removes the need for on-premise equipment and delivers reduced, predictable OpEx
• Reduced Complexity	○ Integrated operations into a cloud-based approach removes the need for a complicated stack of old solutions, reducing Operating effort
• Increased Performance	○ Improves and speed up the access to online resources by utilizing a worldwide network architecture geared for, <ul style="list-style-type: none">▪ Low Latency▪ High Capacity▪ High Availability
• Threat Protection	○ Prevent Cloud and online assaults such as Malware, Cloud Phishing, Ransomware, Malevolent insiders
• Data Protection	○ Secures incoming and outgoing data between public and private networks
• Increased Network Performance	○ Decreases latency and enhances App & Network performance by removing backhauled traffic flows

PLAYERS IN SASE MARKET

Magic Quadrant Core players

- **Leaders** - Zscaler, Netskope & Palo Alto
- **Challenger** - Fortinet
- **Niche Player** - Versa



SIFY SASE CAPABILITIES



SASE Core Capabilities

- Secure Web gateway
- Firewall as a service
- Zero trust network access
- Cloud access security broker
- Remote Browser isolation
- Data loss prevention

SASE Recommended Capabilities

- Network sandbox
- DNS Protection
- SAAS out-of-path (API based)
- Web app & API Protection
- CDN, External DNS
- Support for managed and unmanaged devices

SASE Optional Capabilities

- Wi-Fi hot spot protection
- Network obfuscation or dispersion
- Legacy VPN
- Edge compute protection

SASE SCHEMATIC



Sify Add-on

Managed Network & Security Services



Exceptional Experience

SASE provides performance, integration, security, and management across your network for an exceptional experience for all users, applications, devices, and locations.



NETSKOPE

Why Netskope?

BENEFITS

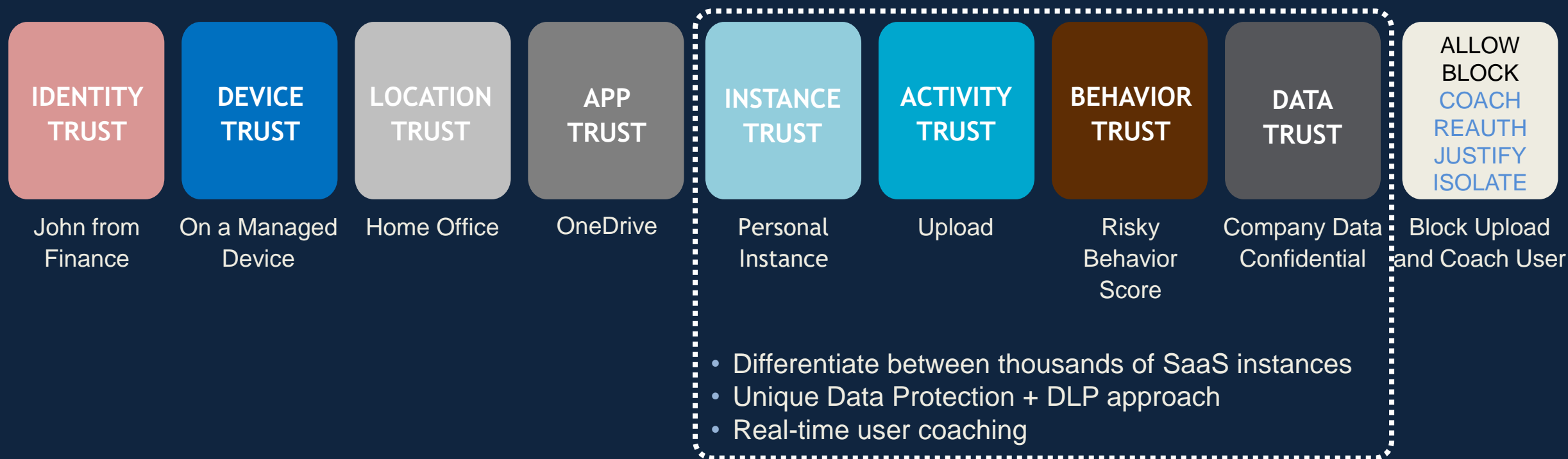
- Zero trust for web, SaaS and private apps
- Unmatched SaaS visibility and control
- Superior traffic inspection
- AI-powered security
- Best-in-class data and threat protection
- Full-path visibility and remediation

ULTIMATE VISIBILITY AND PROTECTION



NETSKOPE ZERO TRUST ENGINE

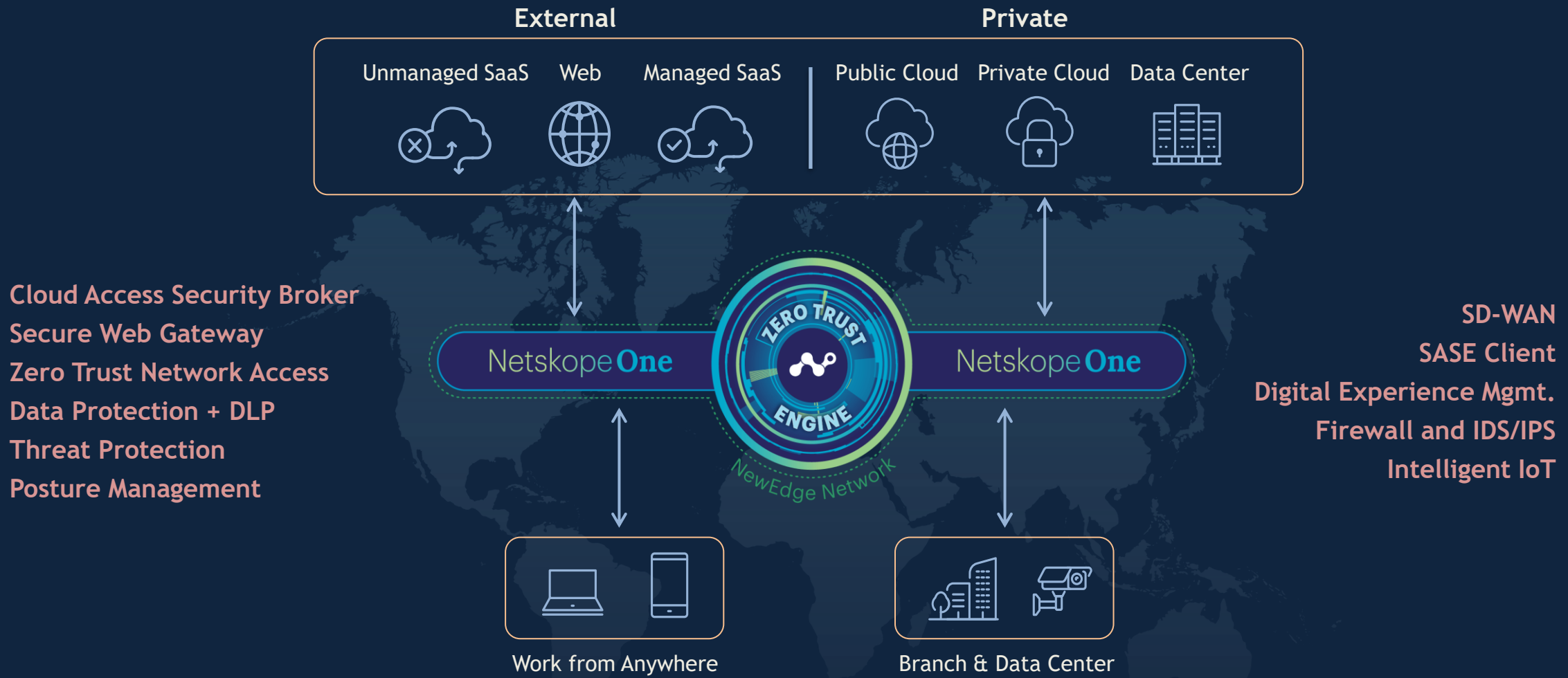
MAKE CONTINUOUS, ADAPTIVE TRUST-BASED POLICY DECISIONS IN REAL-TIME



60% of traffic is SaaS and cloud, delivering 50% of threats

95% of traffic is encrypted—where threats and data hide

NETSKOPE SASE



NETSKOPE SASE



Next Gen Secure Web Gateway (SWG)

Netskope Next Gen Secure Web Gateway delivers web security from the cloud, protecting cloud services, applications, websites, and data for any user, location, or device.



CASB

Netskope's industry-leading cloud access security broker (CASB) solution enables you to quickly identify and manage the use of cloud applications, regardless of whether they are managed or unmanaged.



NPA (ZTNA)

Netskope Private Access, a Zero Trust Network Access (ZTNA) solution, seamlessly connects authenticated users anywhere, using any devices to private resources in data centers and public cloud environments.



Cloud Firewall

Netskope Cloud Firewall (CFW) provides network security on outbound traffic across all ports and protocols for users and offices.

NETSKOPE SASE



Data Loss Prevention

Consistently discover, monitor, and protect sensitive data across every network, cloud, endpoint, email and user.



Device Intelligence

Enforce zero trust device security through discovery, risk assessment and management of internet-connected things in the industrial and enterprise networks.



Remote Browser Isolation

Isolate uncategorized and risky websites for safe viewing all within one cloud platform, one console, and one policy engine.



SaaS Security Posture Management

Continuously monitor and enforce SaaS security settings, policies, and best practices to reduce security and compliance risks.

NETSKOPE CREDENTIALS



>2,500 Customers | >25 of the Fortune 100



Financial Services



Healthcare Providers



Telecom



Retailers



Engineering & Manufacturing

2 OF THE 4

world's largest

5 OF THE 7

world's largest

2 OF THE 3

world's largest

2 OF THE 5

world's largest

4 OF THE 9

world's largest

ESTABLISHED

Market Leader

Gartner MQ Leader for SSE - 2024, 2023 and 2022
Forrester Wave SSE - Leader- 2024

GLOBALLY RESILIENT

Private Cloud

NewEdge, Netskope global network, has full compute in data centers in over 70 regions

FOCUS ON

Innovation

Over 150 patents, large team of R&D resources and data scientists

GLOBAL

Compliance

Compliant with data privacy and data sovereignty regulations



NETSKOPE ADVANTAGE



BENEFITS

Higher satisfaction
for hybrid workers

Reduce risk of users choosing
less secure options for
performance

Direct-to-net reduces burden
on VPN

Industry Best SLAs



Fast and
seamless access



Full visibility from
user to application



No performance
trade-offs for security



No backhauling



Simplified and
localized experience



Enhanced Application
Performance



70+
Regions



200+
Localization
Zones



3K+
Network
Adjacencies



FULL
Compute



Industry's
Best

THE NETSKOPE DIFFERENCE



DELIVER THE MOST GRANULAR AND PRECISE CONTROLS TO EASILY ADOPT ZERO TRUST



Continuous
Adaptive Trust



Speed and
Resilience



AI-powered
Protection

BENEFITS

↓ 85%

Risk reduction through
the ability to protect data
and stop threats

↑ 20%

Greater workforce
productivity
through **agility**

↑ 50%

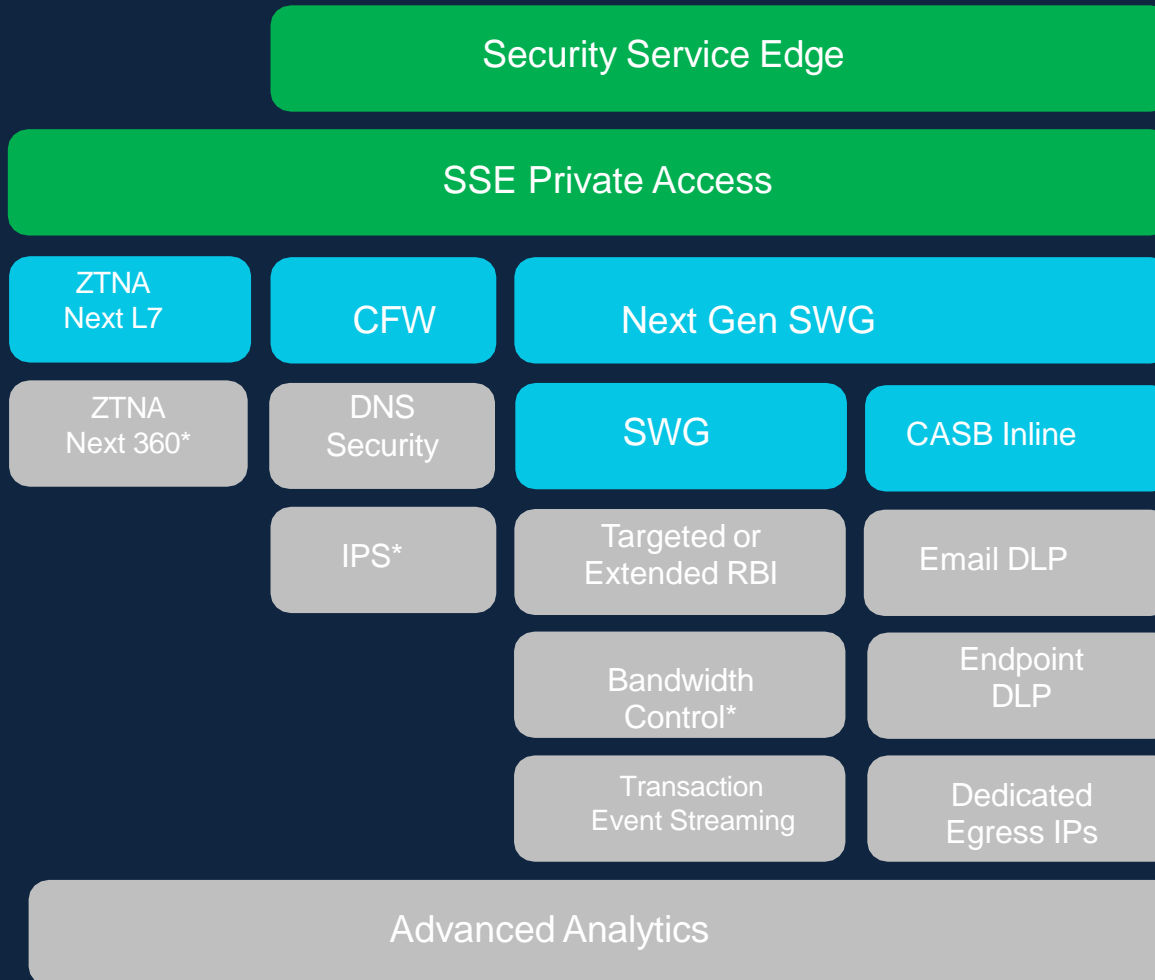
Savings through
**reduced cost &
complexity**

* Results based on data from actual Netskope customers

NETSKOPE LICENSE TIER - INLINE



NETSKOPE SKU'S – PUBLIC AND PRIVATE ACCESS CLASSIFIED AS BELOW:



Packages include when applicable:

- Proactive DEM Standard
- Advanced Analytics Base (7-days)
- Main tenant + Test tenant (upon request)
- NewEdge global access
- Cloud Exchange

Package Add-ons may also include:

- Proactive DEM Professional
- Advanced Analytics (3MR, 6MR, 13MR)
- Customer signed certificates for TLS inspection
- China Premium and Elite access
- Add-on tenants

SASE USE CASE - CHOLA



- Chola was looking for a SASE solution to access the internet and SaaS applications securely and accessing their private/corporate applications without giving access to the whole network and to eliminate the need for separate VPN solution.
- Around 15000 users who will be accessing internet through the provided Zscaler SASE license.
- SASE deployment done with the help of Sify's partner.
- Users will be connecting from the sites ILL/BB using Zscaler client for accessing internet.

#	Zscaler ZPA Feature
1	Private server details
2	Application details
3	Server Groups
4	Device Posture Control
5	Agent Disabled Password
6	SIEM Integration
7	Access policy
8	Group based access policy
9	Timeout Policy
10	Client-less Access
11	Application Discovery
12	Multiple IDP

#	Zscaler ZIA Feature
1	Malware & Advanced Threat Protection
2	IDP Integration
3	Traffic Forwarding Method
4	URL Filtering Rule
5	Cloud APP Control (APPLICATION CONTROL)
6	SSL Inspection
7	File type Control
8	Client connector Agent update policy
9	Tunnel 2.0
10	Cloud firewall policy
11	DNS Security
12	SIEM Integration
13	PAC File
14	Inline Antivirus & Anti spyware
15	Source IP Anchoring



CUSTOMER USE CASES

GLOBAL HOSPITALITY COMPANY

USE CASE

DevOp Access to Public Cloud (IaaS)

Challenges:

- Remote access to Azure vNet
- Complex routing, backhauling traffic, slowness

Benefit Realized:

- Fast and frictionless connectivity for DevOps. Noticeable performance improvements due to NewEdge.
- **Security** – Lock down access. Only accept traffic from Netskope IP address. Lock down publisher IP for connecting to development resources.
- **Expand usage** – Store managers access to proprietary story management system (web applications).

An American multinational chain of coffeehouses and roastery reserves headquartered in Seattle, Washington. It is the world's largest coffeehouse chain with 32,660 stores in 83 countries, including 16,637 company operated stores and 16,023 licensed stores. It has 191,000 employees worldwide.

SOLUTION SET:

- Next-Gen SWG (SWG + CASB+ DLP)
- NPA (ZTNA)
- CASB API
- Advanced Threat Protection
- Cloud Risk Insights

PROFESSIONAL SERVICES

NPA USE CASE

Employee Access/SCCM, Active Directory Connectivity

Business Drivers: Security transformation, compliance, and data governance

Challenges: Provide secure remote access to a globally distributed workforce

Ecosystem: Fortinet Firewall, Microsoft Azure, Office 365, SentinelOne, VeloCloud

NPA Early Use Cases:

- 1) Connecting end user (corporate-issued) devices to Active Directory
- 2) The need to patch/update Windows devices using SCCM

Benefit Realized:

- Enhanced security posture
- Remote worker experience – Secure access with high performance
- Consolidation and cost reduction
- Alignment on vision and road map – Cloud security that fits their cloud-centric infrastructure of the future

A global media, marketing and corporate communications holding company, headquartered in New York City. With 1500 agencies 65K employees, this global enterprise provides brand and advertising services to over 5000 clients in over 100 countries.

SOLUTION SET:

- NPA Professional
- NG Secure Web Gateway (DLP, cloud firewall)
- CASB API-enabled protection
- Professional service with resident engineers

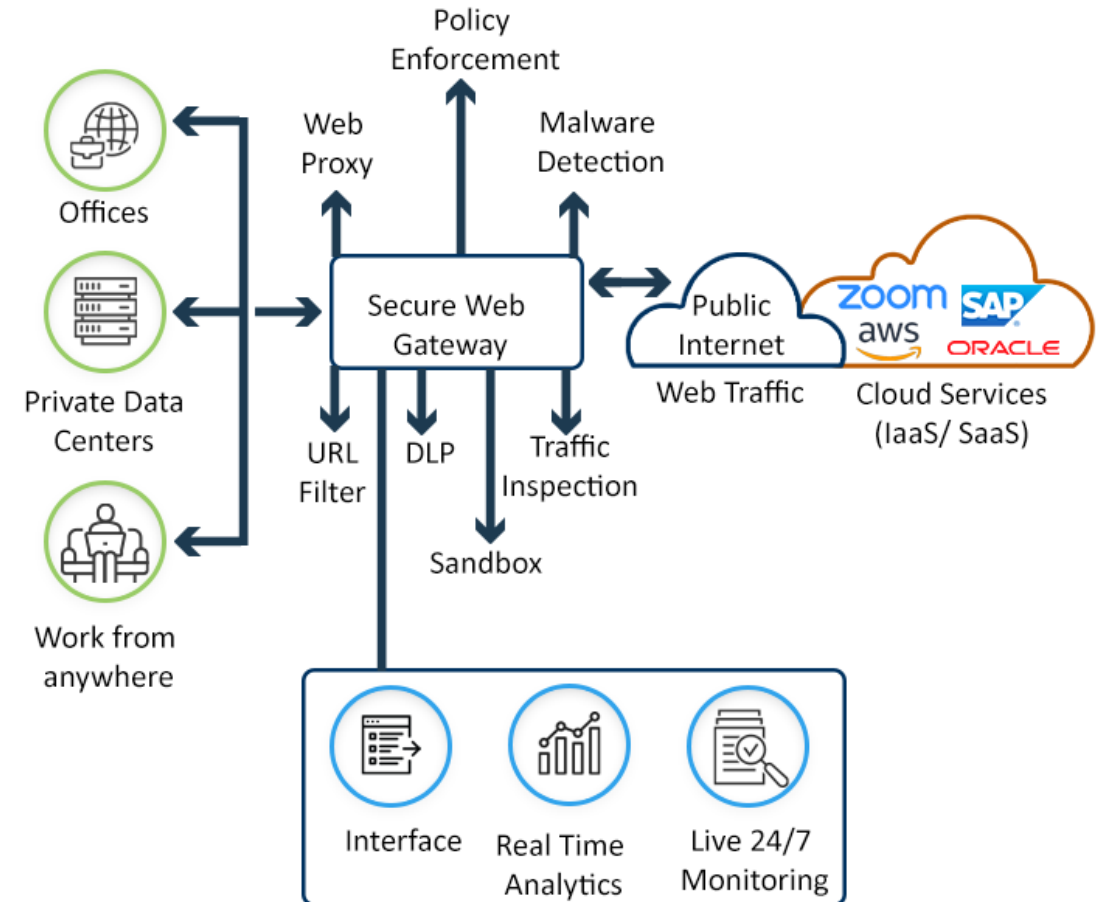
CONCEPTS - SWG

A secure web gateway (SWG) is a network security service that protects company data and enforces security policies.

They also block users from accessing malicious or suspicious web resources.

SWGs are deployed at the boundaries of a network to monitor and stop malicious traffic from entering the organization.

How Secure Web Gateway Works



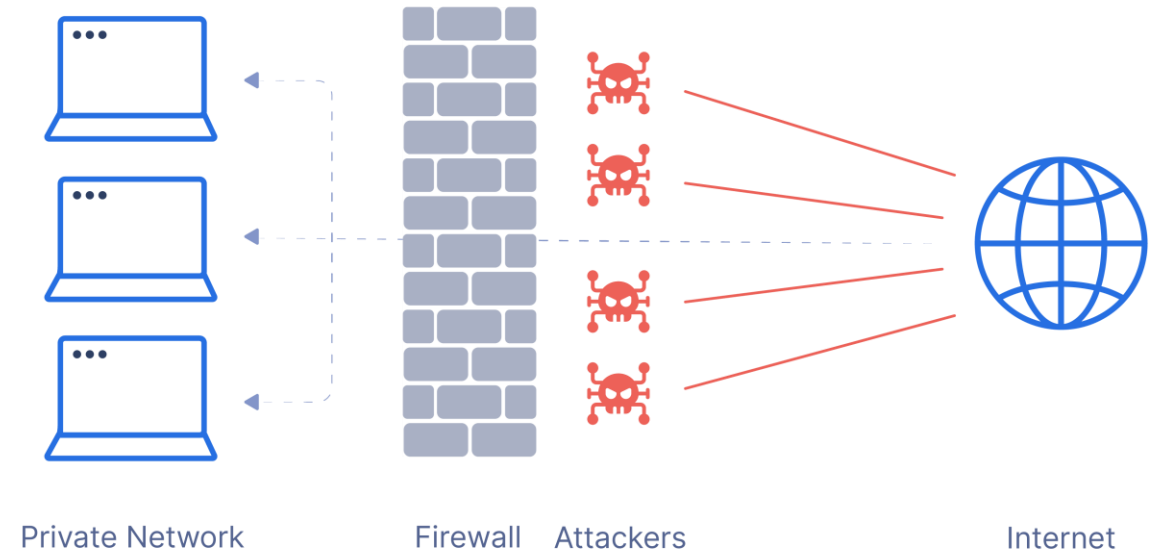
CONCEPTS - FWAAS

Firewall as a Service (FWaaS) is a cloud-based firewall that filters out malicious network traffic.

FWaaS can also provide next-generation firewall (NGFW) capabilities, such as:

- Web filtering
- Advanced threat protection (ATP)
- Intrusion prevention system (IPS)
- Domain Name System (DNS) security

FWaaS is available from traditional firewall providers and cloud-native security companies.



CONCEPTS - ZTNA

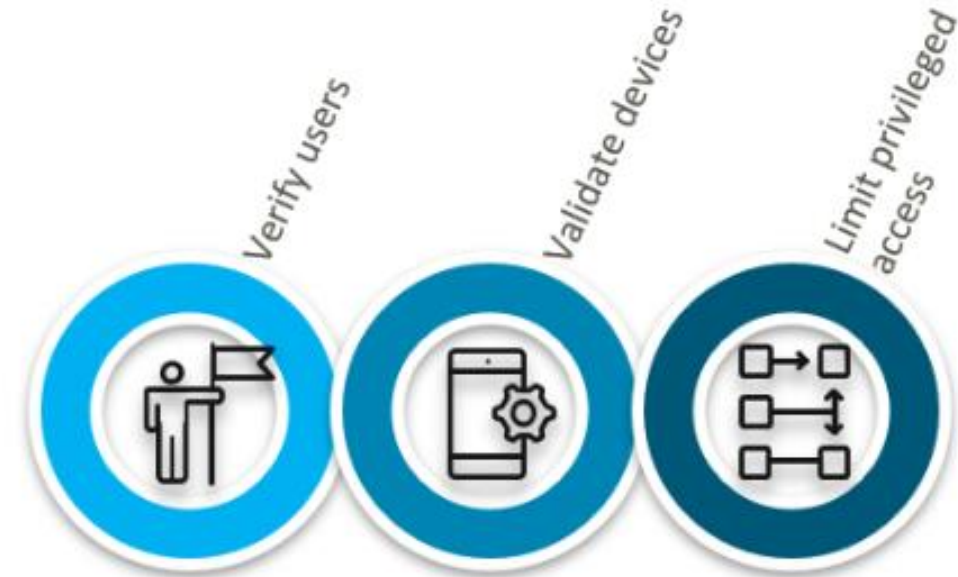
What is Zero Trust?

Castle-and-moat cybersecurity model - anyone outside the corporate network perimeter is suspect and anyone inside gets the benefit of the doubt.

The assumption that internal users are inherently trustworthy, known as *implicit trust*, has resulted in many costly data breaches, with attackers able to move laterally throughout the network **if they make it past the perimeter**.

Instead of focusing on **user and device locations** relative to the perimeter -- i.e., inside or outside the private network -- the zero-trust model grants users access to information **based on their identities and roles**, regardless of whether they are at the office, at home or elsewhere.

Zero Trust Security Model: 3 Steps



- Verify users when they sign on to the system.
- Validate devices before entering the network. Ensure that incoming devices are known, trusted, and up to date on patches and security.
- Limit access based on principle of least-privilege (POLP). The user or device is only given as much authority as needed to access the requested resource, based on roles.

CONCEPTS - CASB

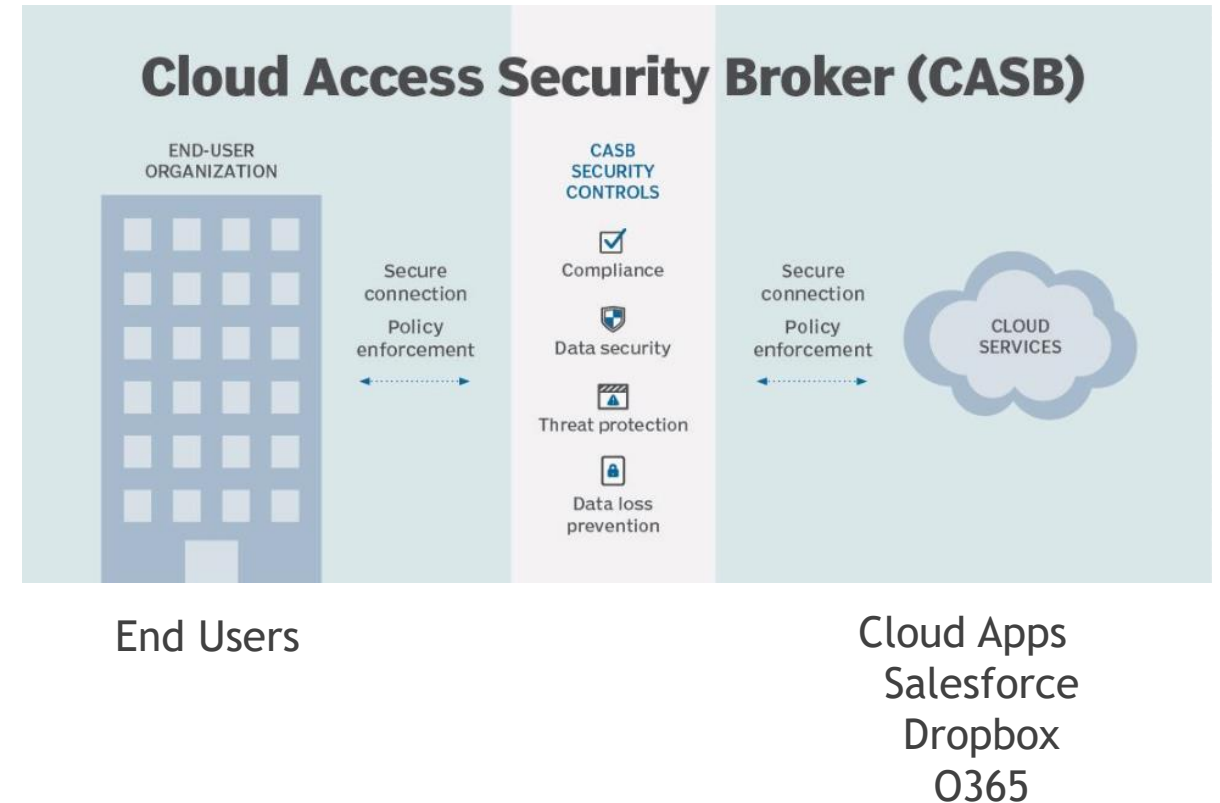


A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure.

CASBs are available as both an on-premises or cloud-based software as well as a service.

CASB acts as a gatekeeper, ensuring the security and compliance of data flowing between an organization's on-premises infrastructure and various cloud services.

By providing visibility, control, and threat protection, CASB enables organizations to confidently embrace the benefits of cloud computing while mitigating the associated risks.



CONCEPTS - DLP

Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

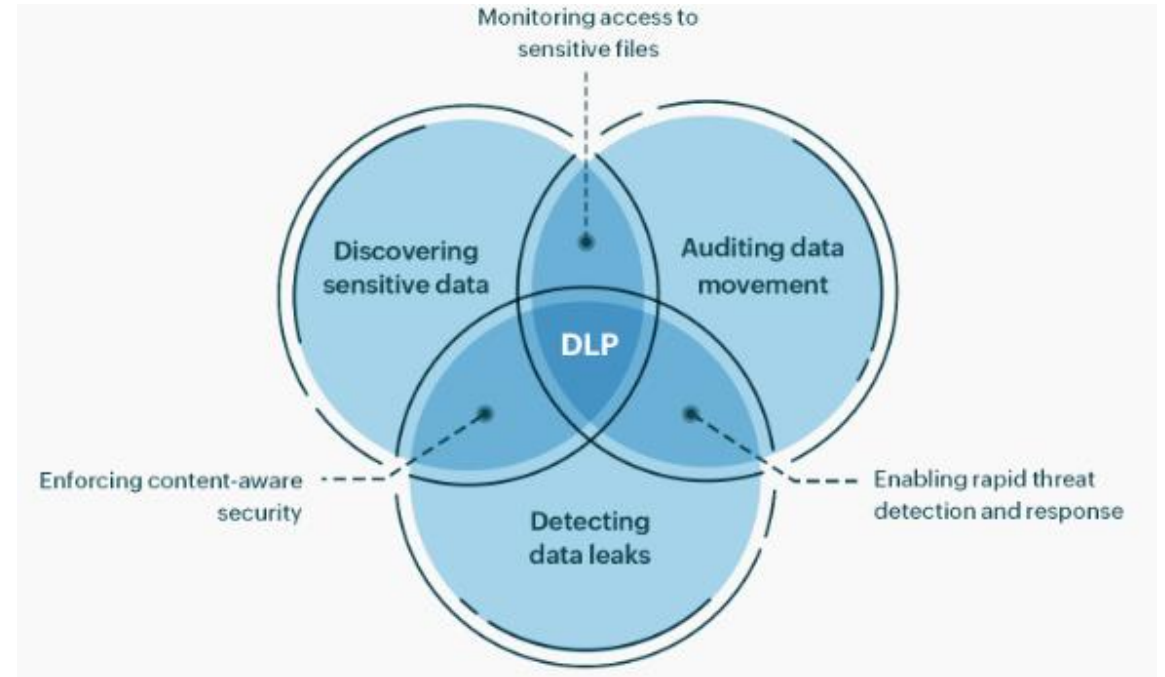
There are three primary types of DLP solutions: network, endpoint, and cloud.

3 Main Uses Cases for DLP

Personal Information Protection / Compliance: Personally Identifiable Information (PII), Protected Health Information (PHI), or payment card information (PCI)

IP Protection: Does your organization have important intellectual property and trade or state secrets that could put your organization's financial health and brand image at risk if lost or stolen?

Data Visibility: Is your organization seeking to gain additional visibility into data movement?



SIFY SASE PROFESSIONAL SERVICES SCOPE



Deployment of dedicated tenant.

Onboarding of users, groups using AD connector or any other method.

Creation & mapping of SWG & Cloud DLP use cases.

Creation & mapping of CASB use cases along with threat protection.

Deployment of ZTNA publisher and mapping of internal applications.

Mapping of a custom policies (if required based on applications).

Mapping of test user group for initial testing and fine tuning of policies.

Support in deployment of end agent on systems of test user group.

Testing of deployed policies along with test user group.



THANK YOU