Transforming the Workplace Security.

Cloud security is NOW.
If you only protect URLs, you are blind to 80% of your traffic.

Think about it, to what extent does your Proxy/ngFW understand what's going on in SaaS?
The Network Inversion

Digital transformation is driving network traffic

**THEN**

- Web Traffic
  - HTTP/S
  - On premises data and users

**NOW**

- Cloud Traffic
  - API/JSON
  - Remote and mobile users

- Cloud apps and services have overtaken web traffic.
- 80% of Web traffic is SaaS.
- 84% of traffic is encrypted.
- **API/JSON** is new language of the internet.

The average enterprise uses over 2400 distinct cloud apps, and don’t know its risk.
Allow/Block strategy generates friction. You can not block O365.
SSL Inspection is key, and many organizations do not inspect all the traffic to Web or SaaS.
1,000 sensitive files open to every employee, and companies can not control where these data go.
Working with appliances introduces high operation costs.
If your users and data are in the cloud, shouldn't your security also be there?

Netskope. Security from the Cloud, offered as a Service. SASE.
Netskope Security Cloud: A SASE architecture

Secure Access to SaaS, IaaS, Web, and Private

Unmanaged Users (BYOD, 3rd party)

Work From Anywhere Users

Offices

Steering Client

ProxyPac

IPSec/GRE Tunnel
Secure Forwarder
Proxy Chaining
SD WAN integration

URLFilter
Sandbox
CASB
UEBA
SSL Insp
DLP
IPS Web
Others...

Web

Public Cloud

Data Center

Private Apps

Security–as-a-service

Network-as-a-service
Decodificación de API/JSON, sobre miles de servicios Cloud.

No vale con allow/block. Hay que entender lo que hace el usuario y aplicar políticas en base a un contexto. Si no decodificas no tienes contexto.
SASE is Security with Context…

Compare it with traditional Internet security…
You can't be SASE without having an EDGE.

Deploying a virtual firewall in IaaS, over a network you don't control, is not going to solve your problem. Netskope, with NewEdge, controls the package from the user to the application.
Netskope New Edge Global Coverage

The most connected network of any security vendor

- Powered by data centers in 40 regions
- Full compute at every location (no reliance on public cloud or virtual PoPs)
- Extensive cloud, CDN & SaaS partnerships with 300+ network adjacencies
- Direct peering with Microsoft & Google at every location
Global Peering: Adjacencies of Notable Networks

The Cloud Security Network most connected

Data sourced from bgp.he.net on June 9th, 2020
Security, even if it is SASE, is a team effort.

Not all the game happens in the cloud. EDR, IAM, SOAR, SIEM are key pieces in this transformation of security.
La arquitectura de seguridad del futuro

Threat Intel Exchange

Endpoint Machines

Response Actions

User & Entity Data

SIEM & SOAR

Response Actions

authentication & SSO

NETSKOPE

Web
SaaS
IaaS/PaaS
Data-Center

IDENTITY

Microsoft

Telefonica

PingIdentity

okta

Google Cloud

Premier Partner

Microsoft Partner

Gold Datacenter
Gold Messaging
Gold Collaboration

12
And now, are you going to continue with your traditional security?

You can keep looking the other way, or take the Netskope pill to control Web, SaaS, IaaS and Remote Access.
Strengths

- Netskope’s vision clearly demonstrates a recognition of the importance of the emerging SASE market, and it is further along in that direction than any other CASB vendor.  

Gartner CASB MQ 2019
Let's make this transformation together.

Gracias