Eleven Paths

SASE:
The future of networks and security is now here

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Executive Summary

Since Gartner published their report entitled "The Future of Security Networks is in the Cloud" in August 2019, which pointed out the concept of SASE as the key to the future of networks and security, there has been a constant and growing buzz around it. But despite everything that has been written since then, we still hear frequent questions such as: What is SASE really? Or, where can I buy it?

The truth is that SASE is not a product or service that one can acquire directly from a provider, but a new model for delivering network and security services. It represents a relevant evolution of trends that have emerged in recent years, such as 'Security as a Service' or 'Network as a Service'. SASE is also intended to cover a huge range of scenarios, technologies and network and security services, so it is not surprising that there is some confusion around this concept.

Below, we will try to clarify the problems that led to the appearance of SASE, describe the model and the benefits for the customer and explain what the keys are to adopting it.

01 The origin of SASE: networks and security are adapted to digital transformation

1 DIGITAL TRANSFORMATION

› **Adoption of the cloud model:**
Up until now, current architectures, in which the DPC was the centralising element of IT, communications and security, have evolved into hybrid and distributed architectures with new formats such as 'Software as a Service' (SaaS), 'Platform as a Service' (PaaS) or 'Infrastructure as a Service' (IaaS).

› **The adoption of work models outside the office:**
General improvements in access to mobile and fixed Internet have facilitated the explosion of teleworking: from any location and with every kind of device

2 SITUATION IN THE FIELD OF COMMUNICATIONS

› **The Internet:**
Reliable, high-speed Internet access is widely available.

› **The software-defined WAN:**
Companies are committed to building their networks using a model that is more flexible and more scaleable, which makes use of both its MPLS accesses and the Internet, and management of traffic flows through policies adapted in real time to the state of the network. It is the launch of SD-WAN technology.

This launch is adapted to the migration of certain traffic from the VPN MPLS to the Internet, caused by the adoption of the IaaS model.

› **Network Function Virtualisation (NFV) architecture**
Virtualising network functions within an NFV architecture provides benefits such as cost reduction when using general-purpose hardware, faster implementation of new network services, and scalability.

› **Remote Access:**
Companies have increased the capacities of their remote access servers as internal demand has grown but they have maintained their centralised schemes, mainly in the area of the DPC.

3 SITUATION IN THE FIELD OF NETWORK SECURITY

› **Security solutions offered from the cloud (Cloud SecaaS):**
We have seen how security providers were also adopting the model of 'Cloud Software as a Service', creating new products or versions of their products focused on protecting cloud environments, giving rise to the 'Cloud Security as a Service' (SecaaS) model.

There are now proxies for browsing and firewalls in the Saas model, and new services have emerged such as CASB (Cloud Access Security Broker, an application for protecting SaaS).

› **Network security functions virtualisation (NFV architecture)**
Network security functions have also appeared in the NFV architecture, and especially in SD-WAN environments, with deployments in the CPE. These functions include firewalls, next-generation firewalls and intrusion detection systems.

› **The security stack in IaaS environments:**
Companies have extended their current network security mechanisms to IaaS environments, deploying new devices in their virtualised versions, or by using services created by the cloud provider itself.

4 THE PROBLEM REVOLUTION VS. EVOLUTION

Digital transformation based on cloud architectures and mobile work models has resulted in a profound revolution, but communications and network security have not evolved at the same rate.

Network architectures that were designed under certain premises that are no longer true have been maintained, and this leads to many instances of inefficiency:

- The DPC (No) is the central point of IT, communications and security itself, around which everything revolves.
- Employees (No) work almost entirely from their offices with their corporate and controlled devices, and (No) use a private network to communicate with corporate applications.

5 THE WEAKNESSES OF THE CURRENT SITUATION

› **Increased complexity of deployment, maintenance and security management:**

With the adoption of public cloud models (IaaS, PaaS, SaaS) and the proliferation of ways to access the Internet in head offices, the perimeter of the company's network increases and is often not even well defined. Deploying independent protection mechanisms at each new point on the perimeter is a complicated undertaking.

Applying the current network security stack (IDS, DLP, URL filtering, vulnerability detection, etc.) to each of the silos results in a problem that is hard to manage and maintain.

› **Increased security costs:**

The deployment of security mechanisms at the new perimeter means increased investment and management costs (more complexity, new specialist profiles required). Nor does the NFV model with deployment of virtualised security functions in the CPE seem to help reduce costs, despite initial expectations.

› **Increased security risk:**

If we consider that each point of the new perimeter over which we deploy protection mechanisms is a link in a chain, then the more they grow, the greater the likelihood that one of them will break (a vulnerability, a configuration failure, an inconsistency in the policy), leading to a security breach.

› **Inconsistency of security policies:**

The need to implement specific mechanisms to cover the new scenarios increases the risk of inconsistency in security policies. The lack of interoperability between different solutions, and often from different providers, jeopardises cross-cutting security objectives, for which collaboration is required. For example, data leak prevention or intrusion detection.

› **Remote access that is not adapted to current mobility patterns or cloud environments:**

Centralised remote access at the DPC is poorly adapted to the characteristics of current network traffic. For example, a user located close to the service to which he wants access might be forced to first go through the DPC, located very far from that service. Traditional remote access solutions are also complex to manage and have weaknesses, because they follow an outdated model of trust in the connection's source IP and they are not sufficiently granular.

02 The basics of the SASE model

02.1. What is SASE?

Security Access Service Edge (SASE) is a "service delivery model" that combines WAN capabilities and network security functions. In reality, SASE does not include any truly novel concepts, but rather confirms the validity of the emerging models of 'Security as a Service' and 'Network as a Service'. It also relies on the integration of both models in a single convergent service, combining multiple network and security functions.

It is also important to note that SASE is always delivered in service mode and its capabilities are accessed through the so-called "Service Edge".

What is the "Service Edge"?

This concept raises certain doubts. This edge could be considered to be outside the customer's facilities, or even associated with the footprint of a cloud provider. From our point of view, the "Service Edge" should be interpreted literally as the point at which the service is accessed.

This edge (a node with its capabilities) may be located in an operator's access network, in a cloud provider, in the customer's facilities, or in any of them as appropriate. The key is that, for the customer, this service access door results in a black box every time, since, as we have said, the solution is always delivered in service mode.

02.2. What are the main features of SASE?

1. Global footprint of nodes:
The existence of a **"service edge" allowing access that is efficient and close** (in terms of networking) to the customer's own footprint.

2. A global SD-WAN capability:
Based on the routing between nodes, the SD-WAN capability should **avoid the problems inherent in the global Internet**, such as high or unpredictable latencies.

3. Distributed security implementation:
The security mechanisms are implemented on the service nodes, **without having to redirect traffic to other nodes for inspection.**

4. A native multi-tenant cloud architecture:
In their proposal, Gartner highlight the importance of **avoiding chaining architecture** of security and network devices.

5. Consolidation of functions:
A SASE-type service must consolidate as many security functions as possible on its nodes. This, together with avoiding models for chaining independent functions, also leads inevitably to a consolidation of manufacturers.

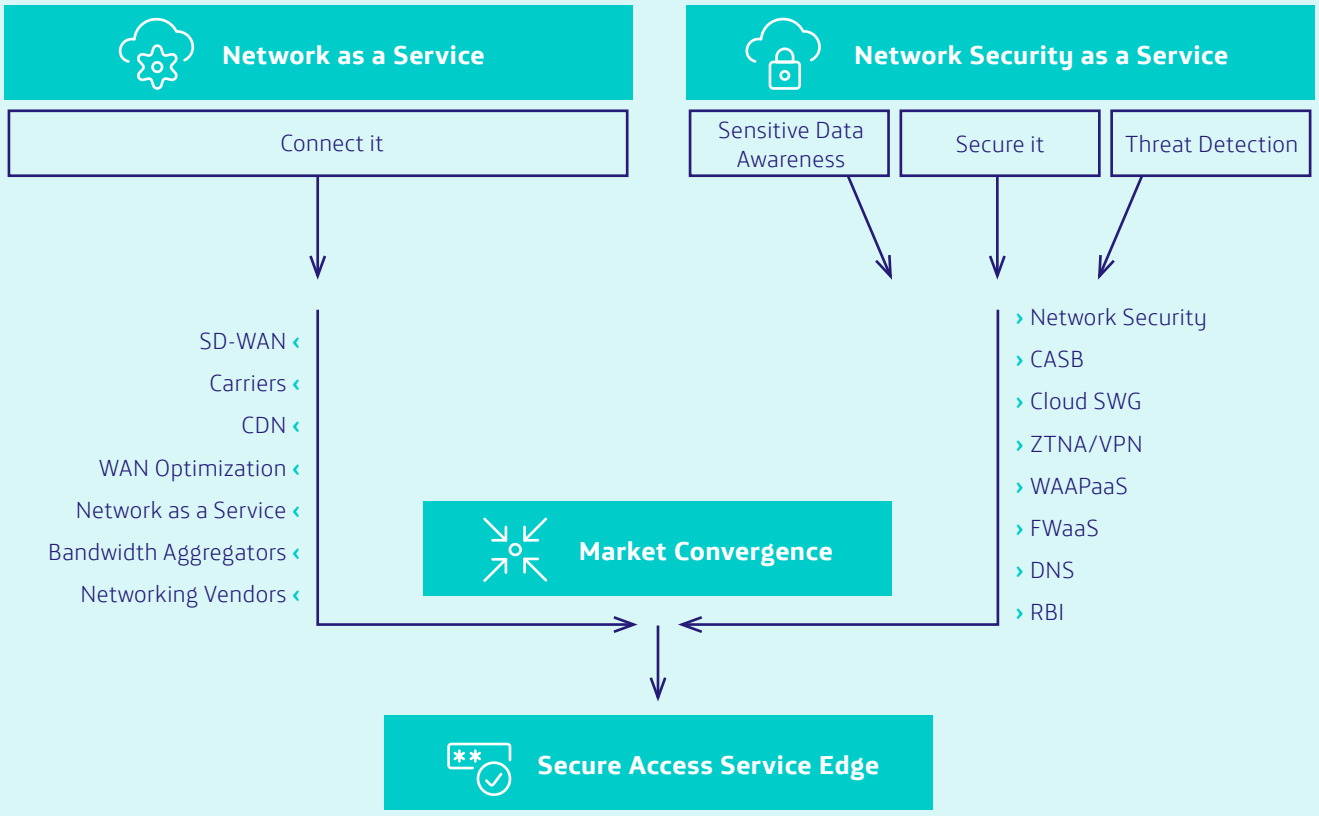
6. Identity as a pillar:
The IP address as a parameter that decides the control of access to a service must disappear, and "identity" must take its place. The identity of the entity that accesses a service must be secured on each connection, and this access limited exclusively to the necessary resources.

This approach is in turn aligned with the Zero Trust Network Access (ZTNA) model that is part of the SASE proposal, and which is presented as an alternative to traditional remote access systems that have security weaknesses and cannot be adapted to cloud and mobility models.

7. Policy-based:
The definition of policies should be the mechanism through which the customer interacts with the service. Any details related to nodes or architecture must be clear to the user.

2.3. Use cases

The following figure, taken from Gartner's own article, shows the network and security technologies that a service built with the SASE model should consider.



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a Service. Source: Gartner

We see in the figure that the catalogue of both security technologies and networks is very varied and can be used to solve different problems.

Consolidating this variety of technologies in a single service allows fundamental security problems to be addressed globally and in a consistent manner. The definition of a reduced set of policies is transferred, in a way that is clear to the customer, to specific configurations in multiple technologies, depending on the scenarios being considered.

Moreover, adopting the SASE model in a gradual process offers the best way to guarantee success. It's not about replacing our entire network and security infrastructure overnight. It is essential to identify and prioritise the problems we want to solve and evolve from there by adding new use cases.

Let's consider some basic security problems as use cases to be solved with the SASE model:

- Detecting and preventing data leaks (DLP).
- Detecting and preventing network intrusions.
- Controlling access to corporate applications.
- Protecting the company's online services.

And now let's take the first of these as an example. There are multiple traffic flows that it would be interesting to control in order to detect and prevent data leaks:

- When employees surf the internet in or out of the office.
- When accessing the company's SaaS applications.
- When remotely accessing corporate applications.
- Or even in traffic travelling between different VPNs of my SD-WAN network.

With a traditional approach we would have different providers and technologies for each of these flows. In a SASE vision, a single service would be able to cover them all, as we gradually incorporated the scenarios.

Internally, the SASE service takes on the job of orchestrating the implementation of DLP policies in the corresponding technologies:

1

Safe Internet Browsing

Secure Web Gateway, Security by DNS, Remote Browser Isolation, FW/Next Generation Firewall as a service, Cloud Access Security Broker

2

Secure access to corporate applications

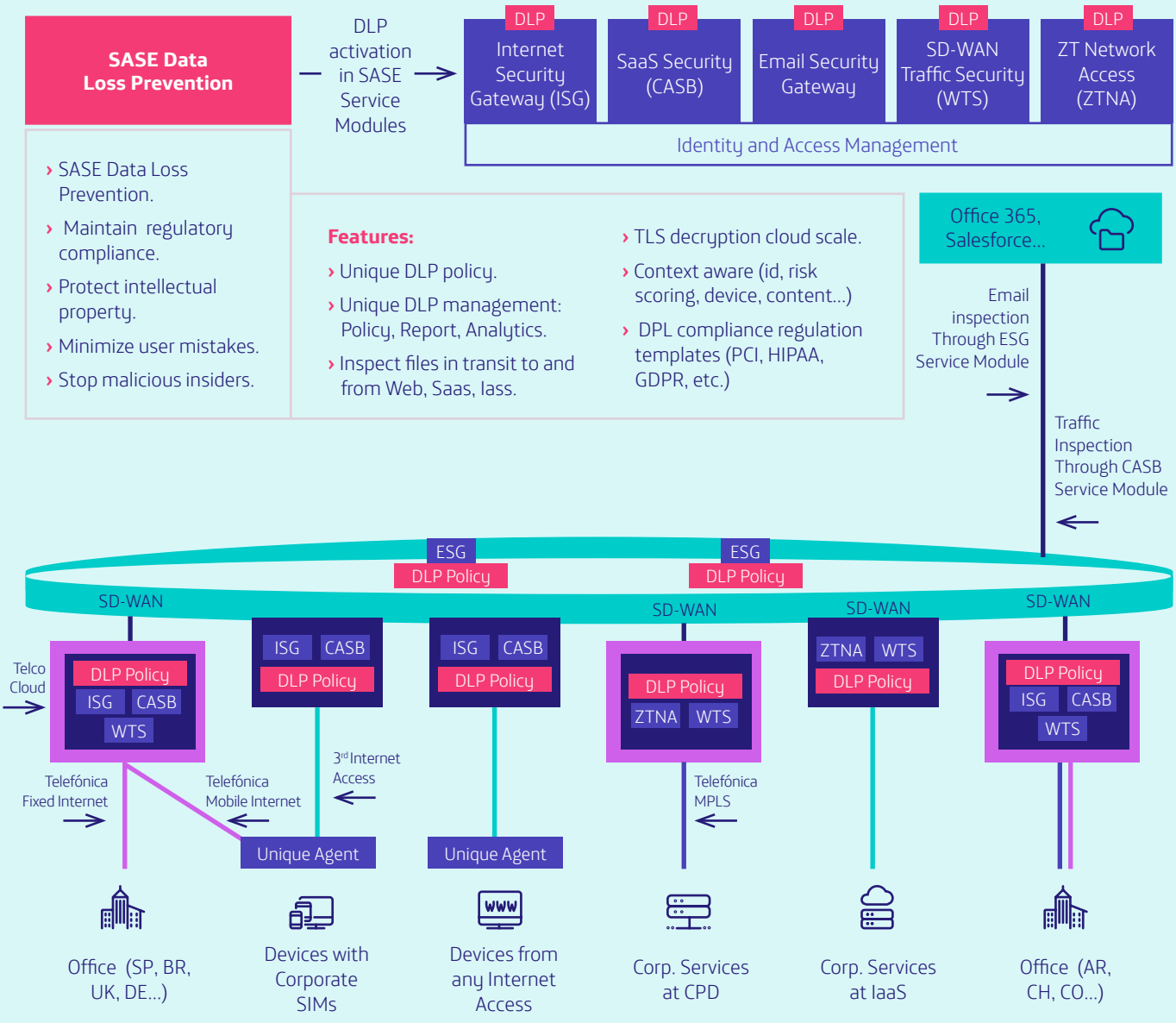
Zero Trust Network Access, Cloud Access Security Broker (SaaS applications)

3

WAN traffic security

FW/Next Generation Firewall as a service, Intrusion Prevention and Detection

The following figure shows how an example like the one described would be implemented, where in addition to seeing the different technologies involved, the way in which the "service edge" is made up of nodes on the Internet and on the operator's own network can be seen. This therefore ensures that all traffic is visible and efficiently managed.



Example of activation of transverse function of Data Loss Prevention on different modules (ISG, CASB, ESG and ZTNA)

We can see that establishing a single DLP policy activates mechanisms in different technologies. This includes the Web Security Gateway module used for employees' browsing, the ZTNA module for accessing corporate applications and, ultimately, all technologies associated with the different traffic flows.

We can also see how the service edge through which the customer accesses SASE capabilities is made up of nodes in the cloud and in the operator's own network, thus ensuring that all traffic is visible and efficiently managed.

03 Benefits for the customer and how their current problems are solved

Here are the main benefits provided by migrating to a SASE model.

Reduced costs

Reduction of security elements, operational load, and the number of providers.

Reduced complexity

Integration of all the components in **a solution built with a native cloud model**, based on the definition of policies and around identity.

Improvements in performance

Optimising the routing of traffic between service nodes should offer better performance and low latency, which is critical for certain services such as video conferencing, VoIP, etc.

Improvements in security

Through the **implementation of a Zero Trust model**, every session is inspected and authorised in real time. The vision becomes more holistic, and unified management reduces the appearance of errors or inconsistencies that create points of attack.

Ease of use for the user

A single agent software should meet all the needs of users and provide a consistent experience regardless of where users are and what they are accessing.

04 Conclusions

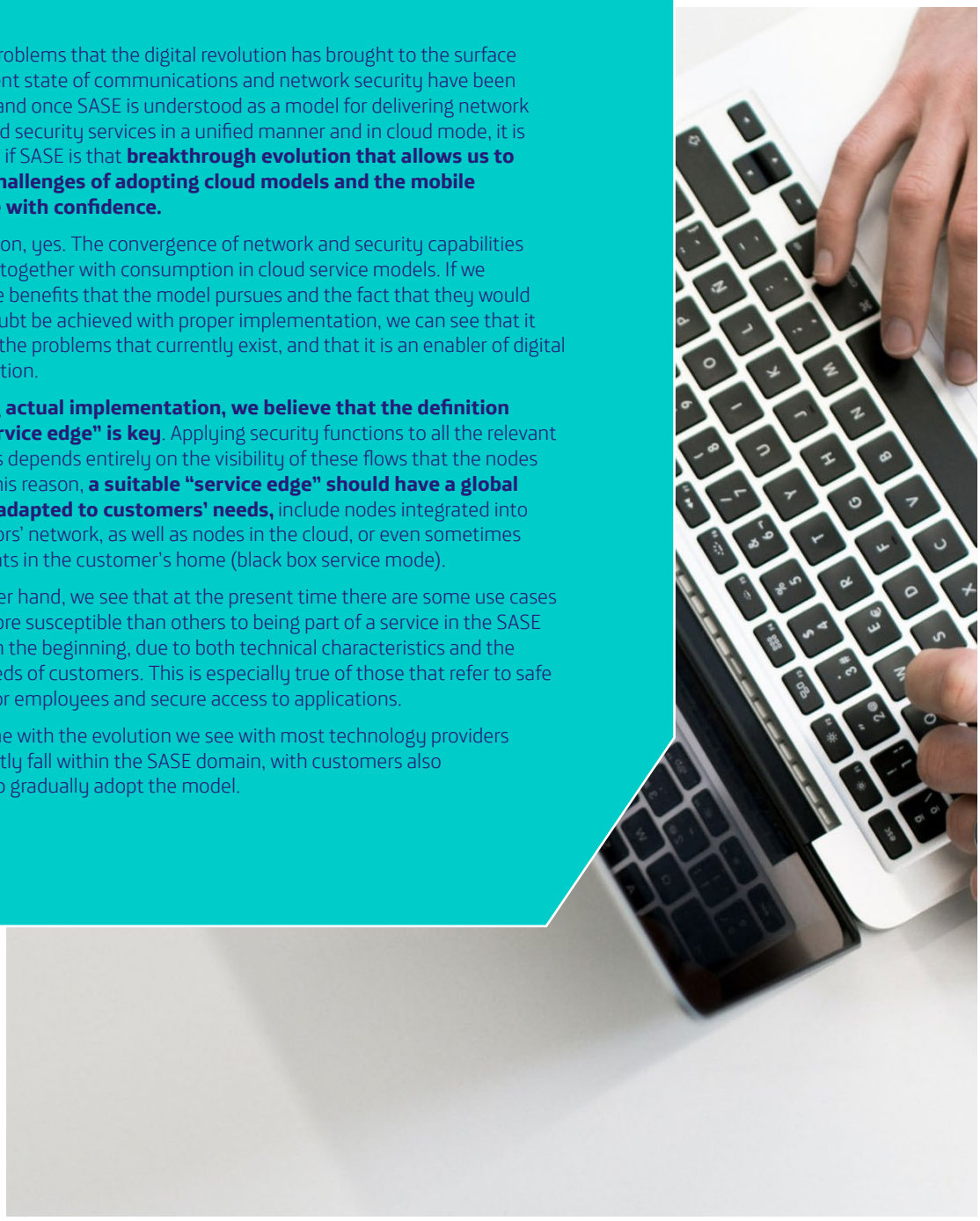
Once the problems that the digital revolution has brought to the surface in the current state of communications and network security have been identified, and once SASE is understood as a model for delivering network security and security services in a unified manner and in cloud mode, it is time to ask if SASE is that **breakthrough evolution that allows us to face the challenges of adopting cloud models and the mobile workforce with confidence.**

In our opinion, yes. The convergence of network and security capabilities is the way, together with consumption in cloud service models. If we analyse the benefits that the model pursues and the fact that they would without doubt be achieved with proper implementation, we can see that it eliminates the problems that currently exist, and that it is an enabler of digital transformation.

Regarding actual implementation, we believe that the definition of the "service edge" is key. Applying security functions to all the relevant traffic flows depends entirely on the visibility of these flows that the nodes have. For this reason, **a suitable "service edge" should have a global footprint adapted to customers' needs,** include nodes integrated into the operators' network, as well as nodes in the cloud, or even sometimes deployments in the customer's home (black box service mode).

On the other hand, we see that at the present time there are some use cases that are more susceptible than others to being part of a service in the SASE model from the beginning, due to both technical characteristics and the current needs of customers. This is especially true of those that refer to safe browsing for employees and secure access to applications.

This is in line with the evolution we see with most technology providers that currently fall within the SASE domain, with customers also expected to gradually adopt the model.



About ElevenPaths

At Telefónica's Cybersecurity company ElevenPaths, we believe in the idea of challenging the current state of security, a characteristic that must always be present in technology. We are continually rethinking the relationship between security and people, with the aim of creating innovative products capable of transforming the concept of security. In this way, we can stay one step ahead of those trying to attack us, who are increasingly present in our digital life.

More information:
elevenpaths.com | @ElevenPaths | blog.elevenpaths

ElevenPaths

Telefónica CYBER SECURITY COMPANY