Orange
Cyberdefense

# SASE: the digital business enabler for your workforce

## Simplifying your network security architecture for the future

# Simplifying your network security architecture for the future

This is a time of unprecedented change for organizations as they shift their services to the cloud, and their employees become more dispersed. To support this new model, the internet is becoming the new corporate network. Traditional network-centric security architecture is too complex to handle this new paradigm. It is becoming a bottleneck that inhibits digital business needs. It’s time for a new security architecture.

## Table of contents

Introduction ........ 3

What is SASE? ........ 4

Why do we need it? ........ 5

Benefits ........ 6

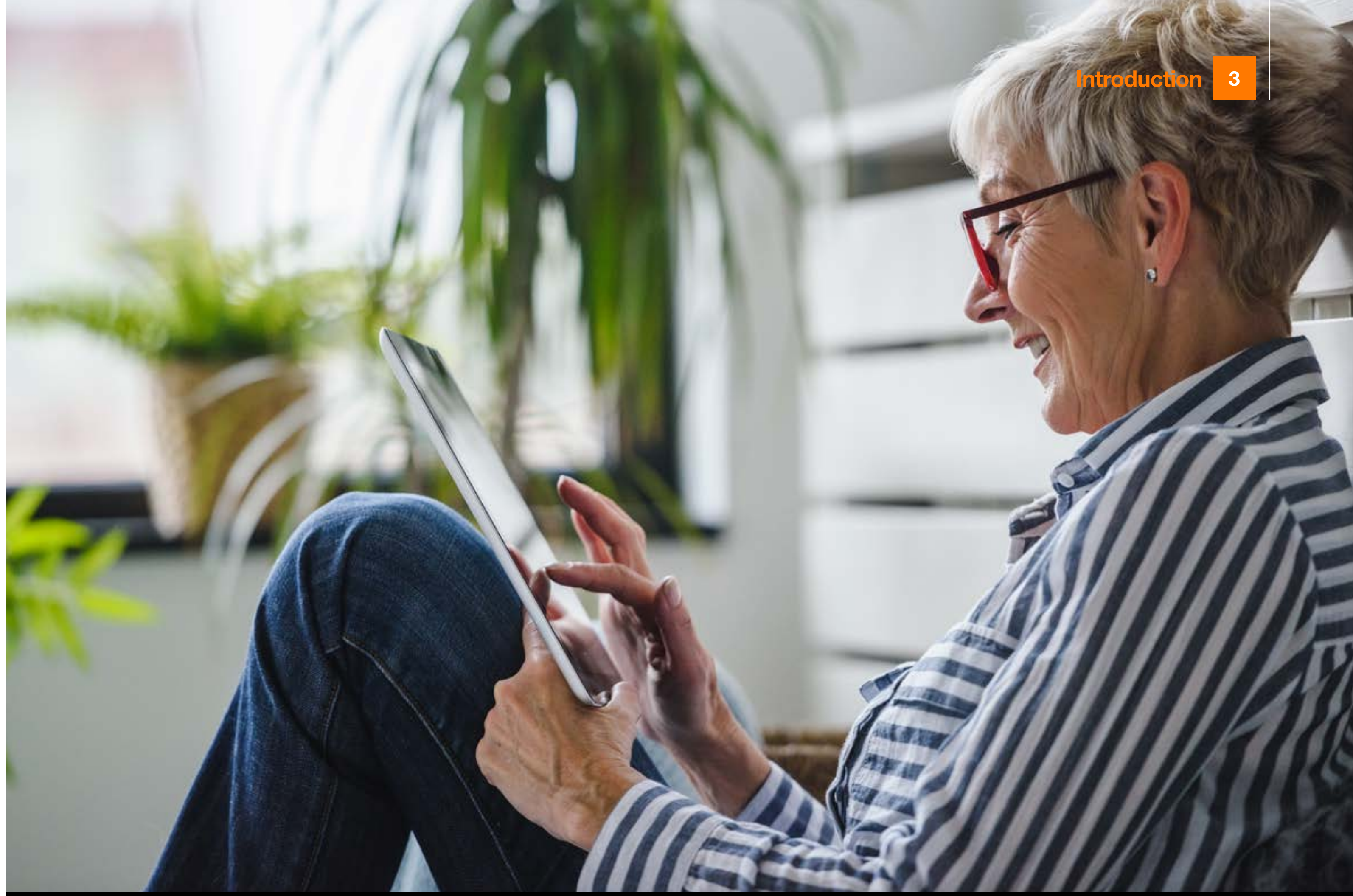
The proposed SASE architecture ........ 8

The importance of identity ........ 13

Guidance ........ 13

Authored by: Peter Mesker, CTO, Orange Cyberdefense Netherlands

With the support of: Etienne Greeff, Group CTO, Orange Cyberdefense, and Thomas Sourdon, Strategic Marketing and Innovation Director, Connectivity Business Unit, Orange Business Services.



## Introduction

**The modern business environment demands secure access to data and applications from anywhere, at any time, from any device, wherever those assets are hosted. The traditional network security model doesn’t support this well. It was built for devices and users that rarely left the shelter of the company network. Those devices were protected by a hard perimeter that protected everything inside.**

Then, users, devices, and applications moved outside the network. The perimeter-based model became less relevant as mobile and cloud computing flung assets far and wide. We needed something more nuanced to replace it.

In August 2019, Gartner proposed a new model known as the secure access service edge (SASE). It reframed networks and network security architecture to help companies cope with the shifting security requirements facing the distributed enterprise.

SASE is a challenging, far-reaching initiative. The market is still catching up to these ideas as vendors struggle to offer the breadth and depth of solutions necessary to support this model.

While we wait for better support from vendors, we can take the opportunity to begin the conversation and engage where we can, monitoring SASE-related market developments and helping our customers to build long-term adoption strategies.

This solution paper explains the SASE model and its benefits, addressing the current challenges. It will guide you as you prepare to embrace this model and secure your digital, distributed business.

## What is SASE?

**SASE is a mindset, not a single product. It unites networking and network security, offering secure access to all users from everywhere.**

It transfers multiple web, cloud, data, and threat protections from on-premises systems to security services that sit at the edge of the wide-area network, close to user locations. This model relies heavily on user identity when granting access to data and applications rather than trusting individual devices or networks.

This new approach redefines the traditional perimeter, replacing on-premises cybersecurity systems with integrated cloud services. It redefines these network security services in software, creating a single platform that can apply unified security policies on a per-session basis for granular security control.

This unified network security ecosystem spans a global network, enabling users to access services consistently and securely from anywhere. It is also extensible, enabling companies to offer more security services as business needs change.

## Why do we need it?

**SASE represents a sea change in the way we approach security, along with a large investment in time and effort. Why would companies pursue it?**

In a world where working practices and infrastructures are facing profound change, organizations must find new ways to stay in control of their data. They must support a new era in which untrusted devices connect to distributed IT resources from uncontrolled networks.

Organizations need SASE to cope with the extra complexity that this creates. It offers an integrated network and network security infrastructure to manage performance and security from a single point using a unified programmable policy. Cloud transformation is a significant driver for the SASE model.

> “IDC predicts that total worldwide spending on cloud products and services will sustain a **15.7%** compound annual growth rate (CAGR) through 2024.[1]

Security services must follow applications and data wherever they go, and they're going increasingly to the cloud. IDC predicts that total worldwide spending on cloud products and services will sustain a 15.7% compound annual growth rate (CAGR) through 2024.[1] SASE's new approach to network security will grow more important as more applications become cloud-native.

> “European Commission figures finding that close to **40%** of workers in the EU switched to full-time telework during the COVID-19 outbreak.[2]

SASE also becomes more necessary as our working patterns change. The pandemic accelerated a growing teleworking trend, with European Commission figures finding that close to 40% of workers in the EU switched to full-time telework during the COVID-19 outbreak.[2] That's a massive increase, given that just 15% of EU workers had ever teleworked before the crisis.

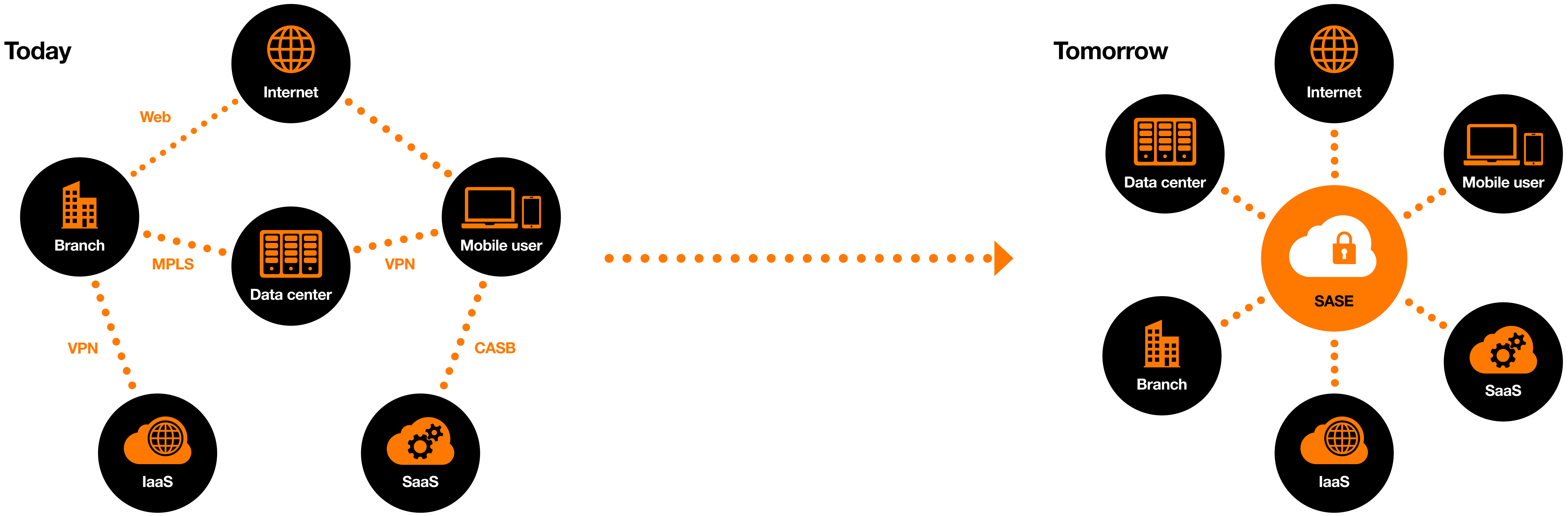
In just a few months, we've already seen gaps in traditional perimeter security as companies struggle to serve a new, remote workforce. For example, the UK's National Cyber Security Centre and the US Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory in April 2020 at the outset of the pandemic warning of several COVID-19 related attacks targeting remote access infrastructure and remote workers' accounts.[3]

In a post-pandemic world, people are the new perimeter. Remote workers need faster, simpler, and more secure access to their applications, even when not using trusted devices. SASE is the key to that secure access.

The growth of IoT is also creating a need for the SASE model. According to IDC, by 2025 there will be 55 billion connected devices worldwide, 75% of which will connect to an IoT platform.[4] That creates a lot of data, which organizations must handle securely. IoT data volumes will increase to 73 zettabytes in 2025 from 18 zettabytes in 2019, the analyst company warned.

This rapidly growing category is accelerating edge access for a flood of challenging new devices. A mixture of high device volumes and equipment with small power and memory footprints makes endpoint IoT security challenging to implement. Moving security to the cloud's edge helps solve these infrastructure volume and complexity problems.

## The future of network security lies in the cloud



## Benefits

**SASE will deliver a rich set of secure network security services in a consistent and integrated manner to support digital business transformation, edge computing, and workforce mobility. Adopting it will deliver the following benefits:**

### Flexibility

SASE allows organizations to direct traffic to the cloud from anywhere rather than routing it via the data center, eliminating a key data bottleneck.

### Cost savings

Putting network security in the cloud helps reduce capital expenditure for on-premises infrastructure. Companies adopting a SASE model will enjoy predictable operating expenditure from a service-based security model.

### Reduced complexity

Organizations can shift security staff from managing individual appliances to delivering policy-based security services from a single point, enabling them to configure end-to-end network and network security structures more simply.

### Increased automation

Software-defined infrastructure is a key tenet of the SASE proposition. It creates a converged technology platform that supports unified policy enforcement programmatically. Just as software developers enjoyed DevOps, administrators can enjoy an automated end-to-end security operations model.

### Better performance

SASE enhances and accelerates access to internet resources via a global network infrastructure optimized for low latency, high capacity, and high availability.

### Zero trust

Zero-trust lies at the heart of the SASE operating model. It offers secure access to private applications in public clouds and data centers instead of access at the network level.

### Threat protection

By putting security at the edge of the network between the user and the cloud, SASE better enables companies to detect and prevent cloud and web attacks such as cloud phishing, malware, ransomware, and malicious insiders.

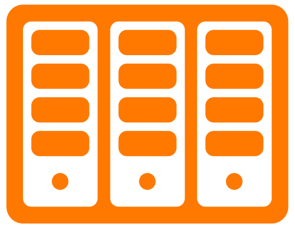
### Data protection

By focusing protection on identity, SASE offers protection at the data level, granting people access to key data assets on a least-privilege basis as part of a strict identity verification process. This protects data everywhere from inside the organization to the public cloud, on untrusted networks, and beyond.

## The proposed SASE architecture

**For years, networks connected users to applications in the data center. These network perimeters used multiple security controls to protect applications and data from outside interference. Organizations sometimes added segmentation to limit the effect of a perimeter breach, along with advanced security appliances inside the perimeter to add extra layers of protection.**

In the early days, the wide-area networks connecting users to data centers used slow, expensive, dedicated lines. Then, several things happened in concert: applications moved to the cloud, edge networking became more prevalent as IoT technology evolved, and the world switched to cheaper internet connections. More recently, users added to these pressures, moving outside the perimeter more permanently as working patterns changed.



### 1 The problem with today's architecture

This perimeter-based network security model can no longer support this environment. In fact, it adds complexity and cost. It still forces connections through the data center even for applications in the cloud, which turns the data center into an expensive bottleneck.

The cybersecurity appliances in the data center are inflexible. They are location-dependent, relying on traffic that passes through a specific network, and they don't scale easily. They rarely use a software-defined control layer, making them complex to configure and difficult to integrate. That makes it difficult to apply consistent, uniform security policies, creating gaps in security posture.

While this model may have worked for office-bound employees, we must rethink it in a pandemic environment that places most employees outside those legacy security controls. We must reassess our incident response plans and re-evaluate responsibility for security in this new work environment.

### 2 How SASE moves us forward

In a modern cloud-centric digital business, users and devices are everywhere, and so are the resources they need to access. We need secure access services everywhere too, built into a global network that is ready to serve users wherever they are.

In this worldwide fabric, container-based security services run in the cloud in edge-based points of presence (POPs). These services include firewalls, secure web gateways (SWGs), cloud access security brokers (CASBs), zero-trust network access (ZTNA), secure DNS, DHCP, and IP address management (DDI).

SASE builds on SD-WAN with additional security features offering end-to-end network protection. This secures data throughout its journey from the user through to the application, regardless of location.

In this model, traffic routes dynamically based on session requirements. It enables direct access to cloud applications without routing through the data center, which reduces latency and load on corporate resources while bolstering security.

This edge-based security model puts cybersecurity services closer to the assets they're protecting. Those assets could be branch offices, but they could also be individual users or even IoT devices. Edge-based network security supports them all.

Identity is key to authentication in this zero-trust network access model. Rather than relying on trusted devices for authentication, these edge-based cybersecurity services focus on the identity of whatever is making the connection.

This approach protects users on insecure home and public networks, not just corporate ones. Users accessing SASE from home networks would typically use an endpoint management agent on their device that would protect it from attack and potentially shield enterprise data from personal assets. However, it is possible to support entirely unmanaged devices by routing them to sandboxed environments via the POP.

> “Identity is key to authentication in this zero-trust network access model. Rather than relying on trusted devices for authentication, these edge-based cybersecurity services focus on the identity of whatever is making the connection.

However, working from home involves broader cultural changes that call for additional security layers. Home networks harbor untrusted devices such as home PCs and smart TVs. Security architectures must acknowledge those.

Organizations must consider what comprises the corporate network in a remote working world. Are employees' homes an extension of the corporate network? Should employers treat threats in the home environment similarly to those in the corporate network? Should they include the home environment in their vulnerability management programs? These are important architectural questions.

3

## Simplifying network

SASE promises more than just security; it promises simplicity. Today's networks are often burdened by a mixture of security products from different vendors. These portfolios grow organically or through acquisition, creating incompatible, complex solution sets that are difficult and time-consuming to manage. They affect network performance and hinder security.

The SASE model consolidates these fragmented cybersecurity environments into a simpler, unified platform involving a smaller set of vendors. That guarantees optimal security everywhere in the network and fosters interoperability, catching threats before they slip through the cracks. It also reduces security tools' impact on performance and cost.

4

## Beyond SD-WAN

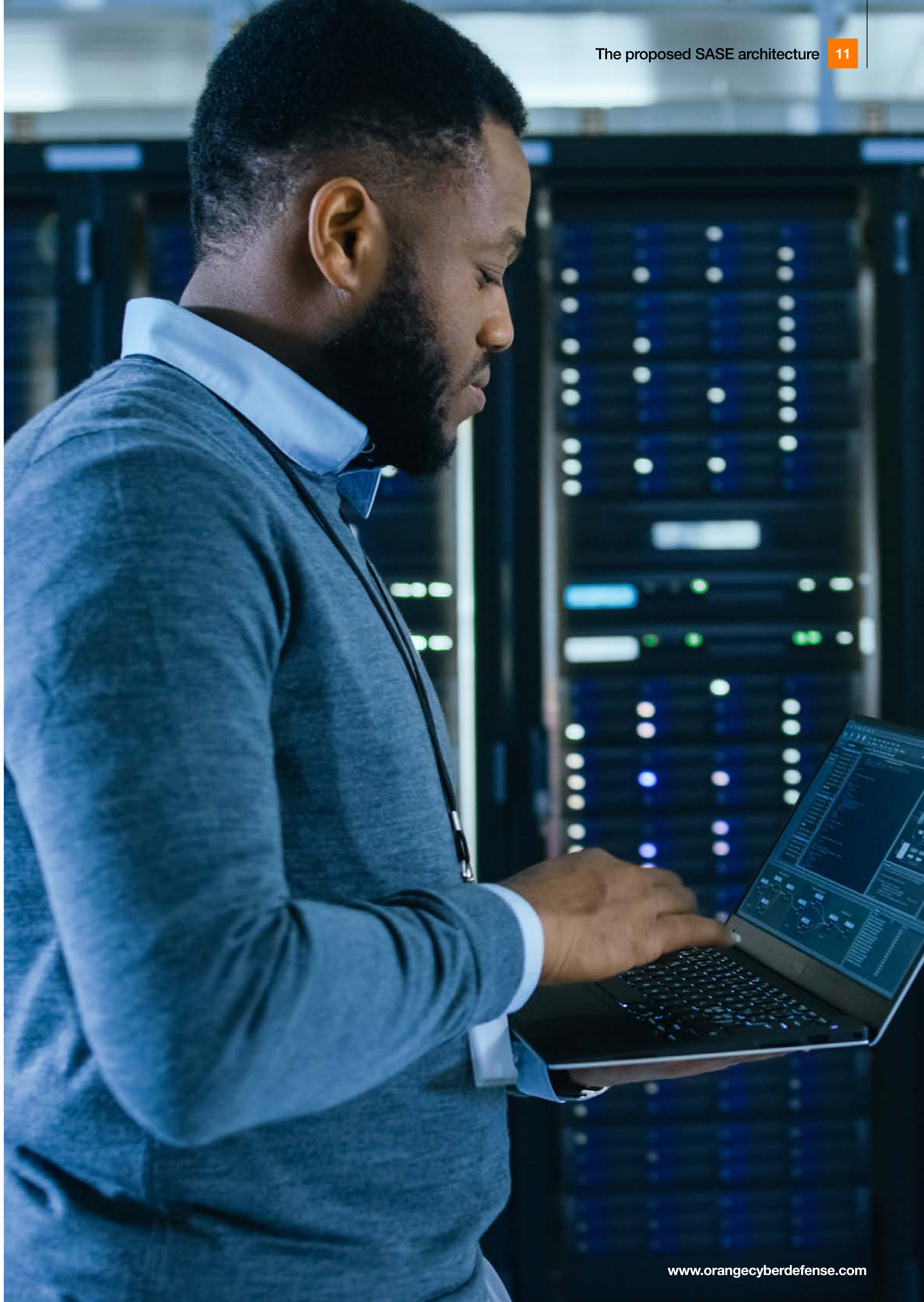
Having spent some time defining what SASE is, it's important to articulate what it isn't. SASE isn't just SD-WAN.

SD-WAN is still a young enough term that vendor implementations vary wildly, making it hard to deliver a reliable and consistent cybersecurity component. Many of them deliver security services via customer premises equipment that can be costly to implement.

Neither is it just cloud-based security. Cloud-based cybersecurity services that don't integrate seamlessly with software-defined network functionality miss out on SASE's zero-trust protection, performance, and uniform security policy advantages.

SASE's marriage of networking and security offers is a simpler, cheaper, and more flexible approach to cybersecurity than thinking about SD-WAN and security separately. Putting cybersecurity services on the software-defined network as cloud-native services on edge-based POPs makes it easier to implement and manage.

> "SASE's marriage of networking and security offers is a simpler, cheaper, and more flexible approach to cybersecurity than thinking about SD-WAN and security separately.



## The importance of identity

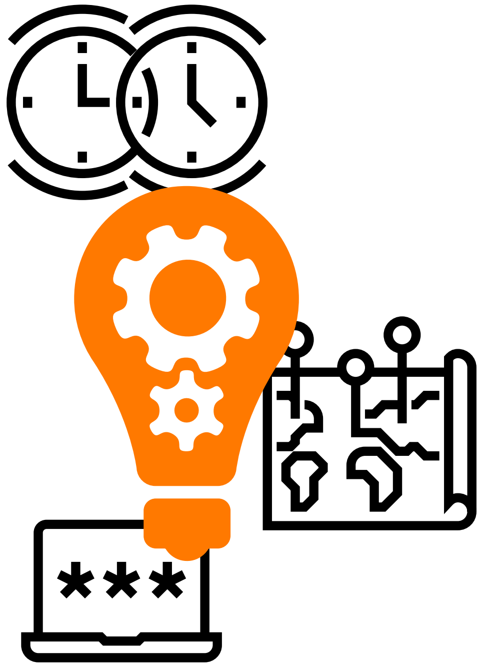
**SASE marries both network and security, delivering both as a cloud-based service, but our focus is on network security.**

Identity underpins those network security services in a SASE environment. This is the key that makes automated policy enforcement possible.

SASE makes context-based decisions when enforcing policies governing security and access privileges. The primary piece of data contributing to that context is the identity of the user, device, or service accessing the resource. Other parameters, including location, access time, trust level, and the data requested, also affect that context.

Because these parameters can all change between sessions, cybersecurity policies adapt on a per-session basis in a SASE environment.

> “Identity underpins network security services in a SASE environment. This is the key that makes automated policy enforcement possible.



## Guidance

**We’ve discussed the ideal SASE environment, but we must be realistic; getting from here to there will involve a lot of heavy lifting. Gartner outlines numerous risks in its report, and many of them stem from the same core concern: a lack of vendor capability.**

We advise you to discuss your long-term SASE architecture plans with security-focused MSPs. Think beyond your technology choices, also considering the security policies and profiles that those SASE-related technologies will support. Dynamic context-based traffic inspection and enforcement - one of the core tenets of a zero-trust network access solution - should be priorities when envisioning a SASE architecture.

A SASE initiative will be a long haul. It redefines how most organizations approach security at a basic level and touches every part of their infrastructure. A mixture of organizational inertia, sunk investment, and technical debt make this project a long-term proposition.

### Stay agile

With this in mind, the move to SASE will be a series of incremental steps. Consider the core requirements of this model when renewing existing projects or implementing new ones, especially around security services such as SWF, CASB, and VPNs.

Look for short-term consolidation opportunities when evaluating these renewals, replacements, and new developments. Now is the time to combine existing services, simplifying, and deduplicating functionality. Explore purchasing decisions from a strategic standpoint, understanding how they will fit into the broader SASE architecture rather than focusing only on isolated product features.

Any purchase or redevelopment is an opportunity to transition legacy services into a software-defined architecture, manageable from a single console. Focus on the destruction of security silos and the integration of products to support unified policies through single-pass inspection.

These architectural decisions will inform the security infrastructure’s ability to scale. They will enhance its adaptability to changing threats and pressures.

## Adopt a mini-platform approach

While a SASE model emphasizes consolidation, we believe it's unrealistic to rely on a single vendor to provide all these moving parts. Even though companies will be able to reduce the number of cybersecurity vendors they work with, they won't be able to procure a single-vendor solution that covers all of their bases.

For example, one requirement of a SASE solution is the inspection of encrypted traffic at scale. This is especially important in an environment that applies multiple cybersecurity protections to that traffic. Not all vendors will support this inspection of encrypted traffic for single-pass, multi-service processing to the level that clients expect.

> “ Clients should push for short-term contracts with flexible licensing when negotiating with vendors to keep their options open during a period of rapid evolution and change.

Other demands on vendors include data context awareness, which goes beyond encrypted traffic inspection to look at how data is being used in a cloud environment. That requires inspection of cloud service provider environments vs application programming interfaces. Not all vendors will achieve this.

Vendors' ability to play nicely in the cloud is also a key concern for Gartner. It worries that vendors with their roots in hardware appliances might have difficulty transitioning to the cloud-native service delivery so crucial in a SASE environment.

Instead of relying on a single vendor, take a mini-platform approach, shrinking their vendor portfolios. Find sets of solutions that rely on between three and five vendors, and replace those with solutions from a single provider. This balances best-in-class capabilities with operational efficiencies.

Clients should push for short-term contracts with flexible licensing when negotiating with vendors to keep their options open during a period of rapid evolution and change.

Even though many of these purchasing decisions won't play out for some time, you can begin challenging vendors now with these emerging requirements and making your buying criteria known. Discuss your technology roadmap with network and security service providers to identify short-and long-term SD-WAN, SWG, CASB, and ZTNA solutions. A focus on integration strategy should be a key part of these conversations because vendors will often build out their SASE offerings via acquisition.

## Drive security from the top

SASE is a cultural initiative, not just a technical one. Its success relies on cooperation from multiple teams across the organization, many of which may be entrenched and ambivalent about change.

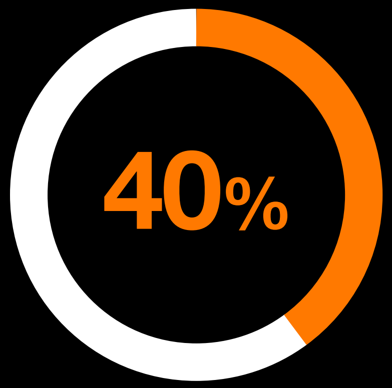
Companies serious about SASE should be willing to drive security from the top, securing buy-in from senior management. Appoint C-suite executives with the power to drive change and overcome political resistance at a team level. Be prepared for the long haul, as this cultural transition will take time, persistence, and patience.

## Involve the CISO from the outset

SASE drives security into the network infrastructure, making it a fundamental component of every corporate workflow. Now more than ever, the security team needs a seat at the table.

The CISO should be involved in all discussions that involve acquiring or transforming a new network or network security solution, internally and with vendors and lead architects. This team should help to evaluate each vendor's offerings and roadmaps.

## A SASE adoption strategy



**Gartner anticipates that 40% of companies will have a SASE strategy by 2024, but there's a long journey between strategy and reality. Companies should begin preparing now for an architectural and cultural change as broad as SASE.**

Indeed, many of them have little choice because the pandemic has forced their hand; they already have to embrace some elements of SASE, such as zero-trust network access in response to the need for remote working. Here are some to-do items for your adoption roadmap.

### 1 Make the business case

Begin by making the case for SASE among key decision-makers. This involves both a long-term strategic case along with smaller, more immediate proposals as part of an incremental deployment.

### 2 Build synergy between security and network teams

Security and network teams often live in silos, but when designing and deploying the SASE model, they can't talk often enough. Begin to build synergy between these groups as early as possible to smooth integration work further along the road.

### 3 Assess the operational and organizational impact on networks and security

When drawing up a long-term architectural proposal for SASE, design teams must consider the operational impact on their systems.

### 4 Begin the SD-WAN transformation

SASE needs a software-defined networking platform for the deployment of edge cloud-based services. This involves moving to an SD-WAN architecture, including the transition from MPLS to internet connections. It is crucial to tackle this stage with software-defined network security services in mind, including a remote access solution in the SD-WAN fabric at an early stage to guarantee consistent security for remote workers.

### 5 Migrate legacy data center cybersecurity services to the cloud

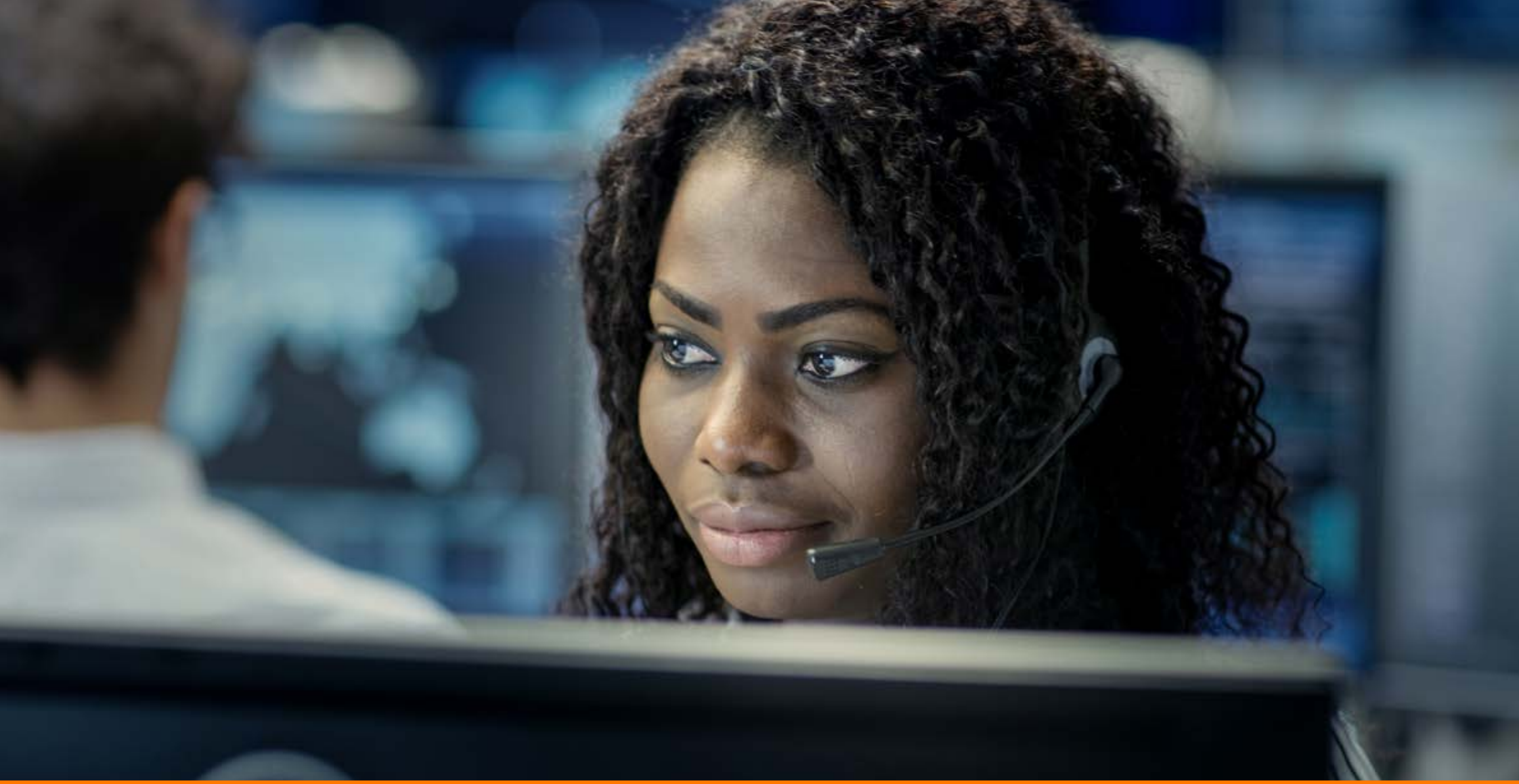
With an SD-WAN solution in place, it's time to plan the move from legacy on-premises security services to cloud-enabled POPs running on the software-defined network. This means transitioning to a cloud security provider.

### 6 Move security posture and design to zero-trust network access

Clients should make the migration to cloud-based security services with zero-trust network access in mind. This includes planning for identity-based access to all applications. Build out components including identity and access management and identity life cycle management frameworks that will support the move to identity-based access. Now is also a good point to consider complementary technologies like multi-factor authentication and device-based network access control to protect managed mobile devices accessing corporate applications.

### 7 Develop an automation framework

With a software-defined network security fabric in place, clients will be well-positioned to drive new efficiencies into their security infrastructure using automation. Invest in creating and refining a software-defined network and security control plane that will form the basis of a robust and adaptive security operation.



# About Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe’s go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat life-cycle.

**Twitter: @OrangeCyberDef**

Sources:
1. IDC - https://www.idc.com/getdoc.jsp?containerId=prUS46934120 European Commission – https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
2. IDC Webinar - Envisioning a Resilient Cloud Based Digital Infrastructure webinar April 2020
3. US Cybersecurity and Infrastructure Security Agencies - https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4. IDC - https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20estimates%20data%20generated%20from,significant%20portion%20of%20this%20data

Orange
Cyberdefense

orange™