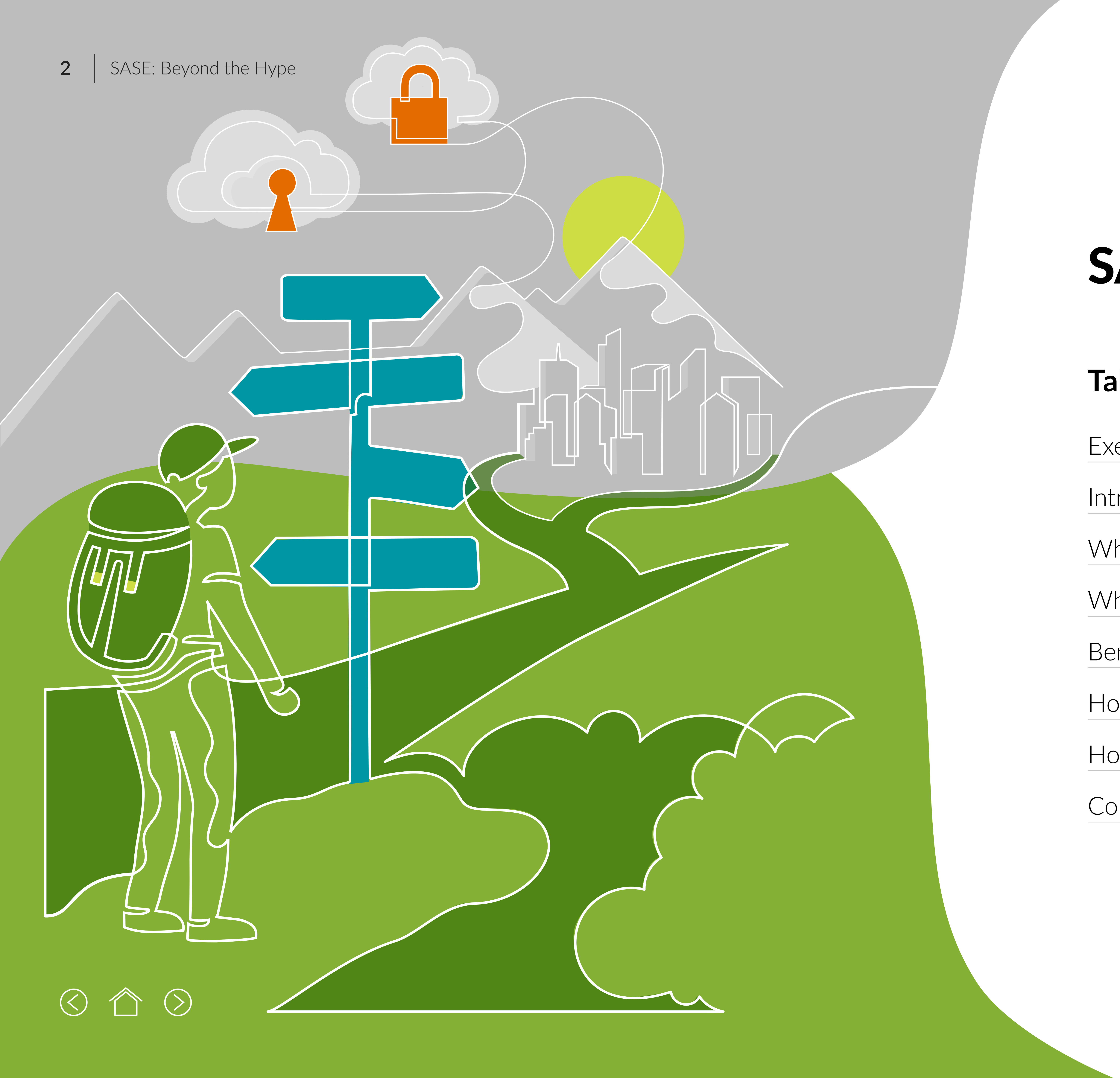
eGuide

SASE: BEYOND THE HYPE

Solve network and security management challenges
with a Secure Access Service Edge architecture

Enter

JUNIPER NETWORKS | Engineering Simplicity



SASE: Beyond the Hype

Table of Contents

Executive Summary

While we've been hearing about Secure Access Service Edge (SASE), Zero Trust Edge, and the journey to the cloud for quite some time, many of us don't know where to begin.

This white paper will help map the journey by explaining what SASE is, why it matters, and the benefits it brings to your network architecture. More than that, it highlights some of the options organizations need to consider, as well as the questions that should be asked before starting the transition to SASE.

Finally, it looks at establishing a blueprint for preparing your organization for SASE, and how to approach this architectural shift.

Introduction

Everyone in information security hears the hype. SASE. Zero Trust Edge. Journey to the Cloud. But what is the hype all about? And why does it matter?

Contrary to popular belief, the perimeter hasn't disappeared. The perimeter is elastic, expanding and contracting in line with constantly changing business requirements.

Wherever users are, services and applications must be accessible and secure. IT security personnel must manage access to cloud applications and services with agility, elasticity, and security.

In Q4 2019, a significant shift in the market emerged: investment in cloud infrastructure jumped 37% year-over-year[1]. This trend provided indisputable evidence that business interest in moving on-premises technology investments to the cloud was accelerating as a strategy. Cloud was already a very healthy segment, and as we began 2020, the momentum of the cloud skyrocketed.

A cloud architecture makes sense for many; after all, there are many advantages to using the cloud. Its operational simplicity, compelling economics, improved service experience, increased agility, and scale provide the flexibility required to meet many business needs.

It helps maintain business continuity and access to services, no matter where an organization's workforce or customers are located.

Organizations require predictable and reliable connectivity coupled with robust information security to protect devices and data. For many organizations, the best option is to leverage the power of the cloud to effectively support both on-premises and distributed workforces, ensuring the best possible experience for all.

That brings us to SASE.

[1] Canalys. (2020, February 4). Global cloud infrastructure market Q4 2019 and full year 2019 [Press release]. https://www.canalys.com/newsroom/canalys-worldwide-cloud-infrastructure-Q4-2019-and-full-year-2019

What is SASE?

In 2019, Gartner coined the term Secure Access Service Edge, better known as SASE, which centers around granting secure access to users based on the risk they introduce at that moment. SASE is the embodiment of networking converged with security. It provides protection from attack, regardless of where users are located, ensuring consistent security enforcement wherever they are without having to backhaul traffic to a corporate location.

Assessing risk is complicated because it is dynamic. Risk posture constantly changes as users, devices, and applications connect and disconnect. To balance and manage risk, organizations must first understand their digital footprint and how applications, services, and users interact and operate. Visibility into and monitoring of these interactions make it possible to identify security weaknesses and potential attack vectors. Without a doubt, this is a complex task to manage in real time.

With SASE, there is more flexibility to respond to risk posture in real time vs. having to anticipate business needs years in advance. On-premises environments lack the ability to quickly adapt to changing business requirements. If more resources are needed to scale up, it may take a considerable amount of time and effort to determine what infrastructure is needed and get it deployed, increasing the risk that the business opportunity will diminish.

Currently, most organizations have to backhaul traffic to the data center through their security stack in on-premises environments. Data may have to travel around the world to reach the inspection point within the data center.

With cloud-delivered security services, it's easier to secure services with very low latency because inspection is geographically closer to the user, and traffic does not need to be rerouted. The data no longer has to travel around the world before the user gains access.

Traditionally, network security has lived at the network edge within corporate walls and in the data center, with all traffic needing to be routed through it for inspection. A SASE architecture moves most of these capabilities to the cloud, where many applications already reside, reducing the distance between the user and application and—in some instances—eliminating backhaul requirements.

Simultaneously, analytics and threat intelligence provide the insight and ability needed to act on threats or prevent risky behavior by users or devices from infecting the network. As security and the network have converged, it has become even more critical for IT teams to use all connection points to see, automate, and protect the network from malicious activity, instead of being restricted to performing these tasks at the data center gateway or physical perimeter. When organizations empower the network to be threat-aware—detecting risks and stopping them from gaining a foothold within the network—safeguarding users, applications, and infrastructure becomes easier. SASE delivers the threat-aware network for the cloud era and should ultimately improve security while reducing complexity and streamlining management. SASE makes security easier to manage and enhances the operational feasibility of the network.

Why SASE Matters

Connectivity should be fast, reliable, and secure. The flexibility of a SASE architecture is a game-changer because it delivers on the value of what a cloud-driven network can do and frees organizations from the limitations inherent in static environments.

Let's use a big box retail store as an example. There is an expectation that network traffic will increase both in-store and online during certain holidays.

The demands on the network require additional resources to accommodate spikes in secure connectivity and to support access with minimal latency.

Traditionally, IT teams invest a lot of time and money in preparing for the increase in traffic and expected barrage of cyber attacks. They are forced to make tough decisions between accessibility (because additional load time for employees and shoppers means lost revenue) and security (because spikes in expected network traffic and online activity directly correlate to spikes in cyber attacks, which also means lost revenue).

In such a traditional architecture, traffic needs to be backhauled to a centralized network hub for security inspection and then routed to the desired application or service.

A SASE architecture provides traffic inspection and makes services accessible to and from points of presence near the geo-location of each physical store and online shopper. Extra resources can be automatically added to accommodate peak demand and scaled down when demand decreases. Businesses no longer need to choose between security or accessibility due to the elimination of backhauling the traffic, making the end-user experience seamless and reducing risk.

SASE delivers networking and security together as one cohesive service, and addresses network and security management challenges for organizations.

Many security controls are equipped with their own security management system, each of which comes with its own configuration and interoperability challenges. These challenges can produce visibility gaps, especially when an integration breaks down or stops working, increasing risk and keeping administration teams busy. But SASE is not a crystal ball and cannot solve these visibility gaps by itself.

Just because these challenges are addressed at the edge does not necessarily mean they will be addressed in an on-premises infrastructure.

Businesses need a strategy to rationalize event and threat detail, including how to sync configuration policies across environments and troubleshoot a service that impacts web applications, employees, and customers.

While organizations can outsource their policy administration when using SASE, they can't outsource their responsibility to address business risk. They are ultimately accountable for what happens on their network, regardless of who manages the day-to-day operations of the network environment.

Although the cloud is where many organizations have set their sights for the next few years, dependence on hardware will not completely disappear. On-premises devices are likely to stay in the local data center, especially for larger enterprises with highly sensitive and custom applications.

A well-built SASE architecture accommodates secure access to services residing in public and private cloud environments simultaneously, while ensuring consistent security policy through a single management interface to avoid configuration mistakes and visibility gaps.

Organizations should incorporate physical, virtual, and public cloud data center environments as part of their SASE initiatives.

Benefits of SASE

Reduced complexity/operational agility

Visibility across the entire environment is critical to quickly assess application and network health, as well as identifying potentially malicious activity. By reducing complexity, existing resources can do more and see farther than ever before. The natural convergence of the network with security capabilities provides one clear focal point. Policy consistency reduces configuration errors and enhances security efficacy.

Ease of use

Historically, security has been complicated. Organizations have had to deal with routing traffic through multiple layers of defense and primary "choke points" where firewalls are situated. There have been many other controls to manage, but with SASE the focus is on the direct connection from client to cloud.

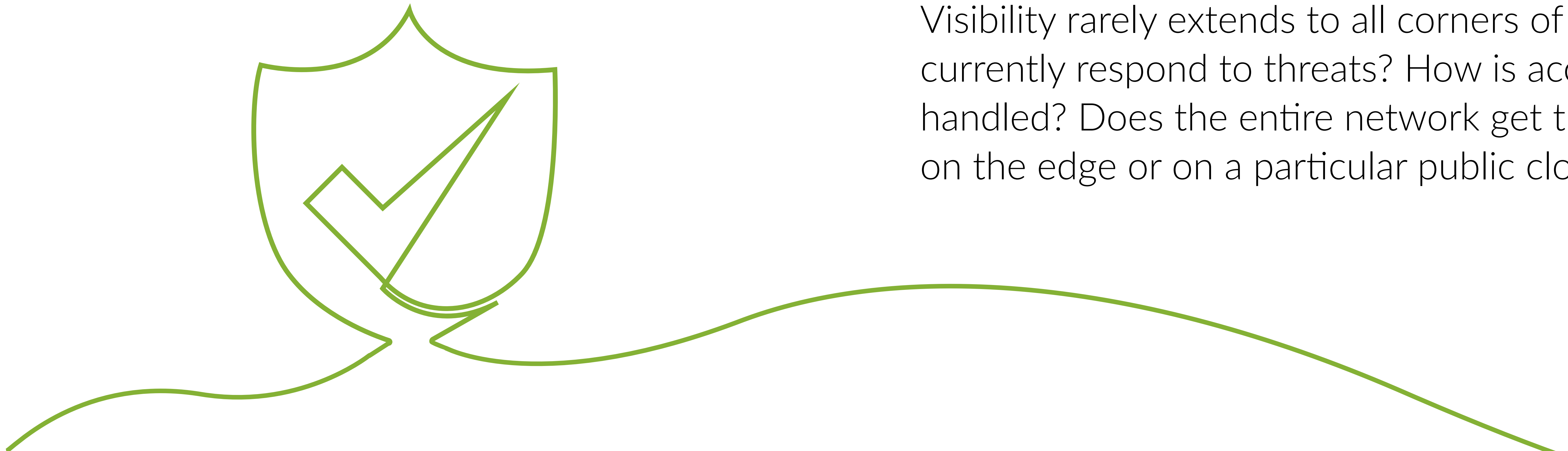
Improved security

Bad actors will use any means necessary to attack the network. Therefore, it is critical to have consistent security policies and services across the network to safeguard users, infrastructure, and applications wherever they reside. SASE delivers vastly improved security that is easier to deploy, and leverages connection points to apply security policies and enforce threat prevention.

How to Prepare for SASE

Adopting a new technology often involves planning, careful consideration, and stakeholder alignment. Downtime is costly: whether it's a loss in employee productivity, delay or loss of customer transactions, or a student missing out on a lesson, it can have a devastating impact on business. There are many obstacles and minimal room for errors that introduce risk, especially when organizations move quickly and under stressful circumstances.

Moving from a physical on-premises environment to one that is mostly cloud-hosted is a big undertaking. It is essential to ensure connectivity, performance, operational monitoring, and administrative controls while keeping business continuity and managing existing infrastructure that will likely remain in use for quite some time.



Here are some key questions to ask regarding the state of the network. When thinking about the advantages of a SASE architecture, evaluate what's right for the organization today, tomorrow, and years into the future. Start with these considerations:

Where is the data today?

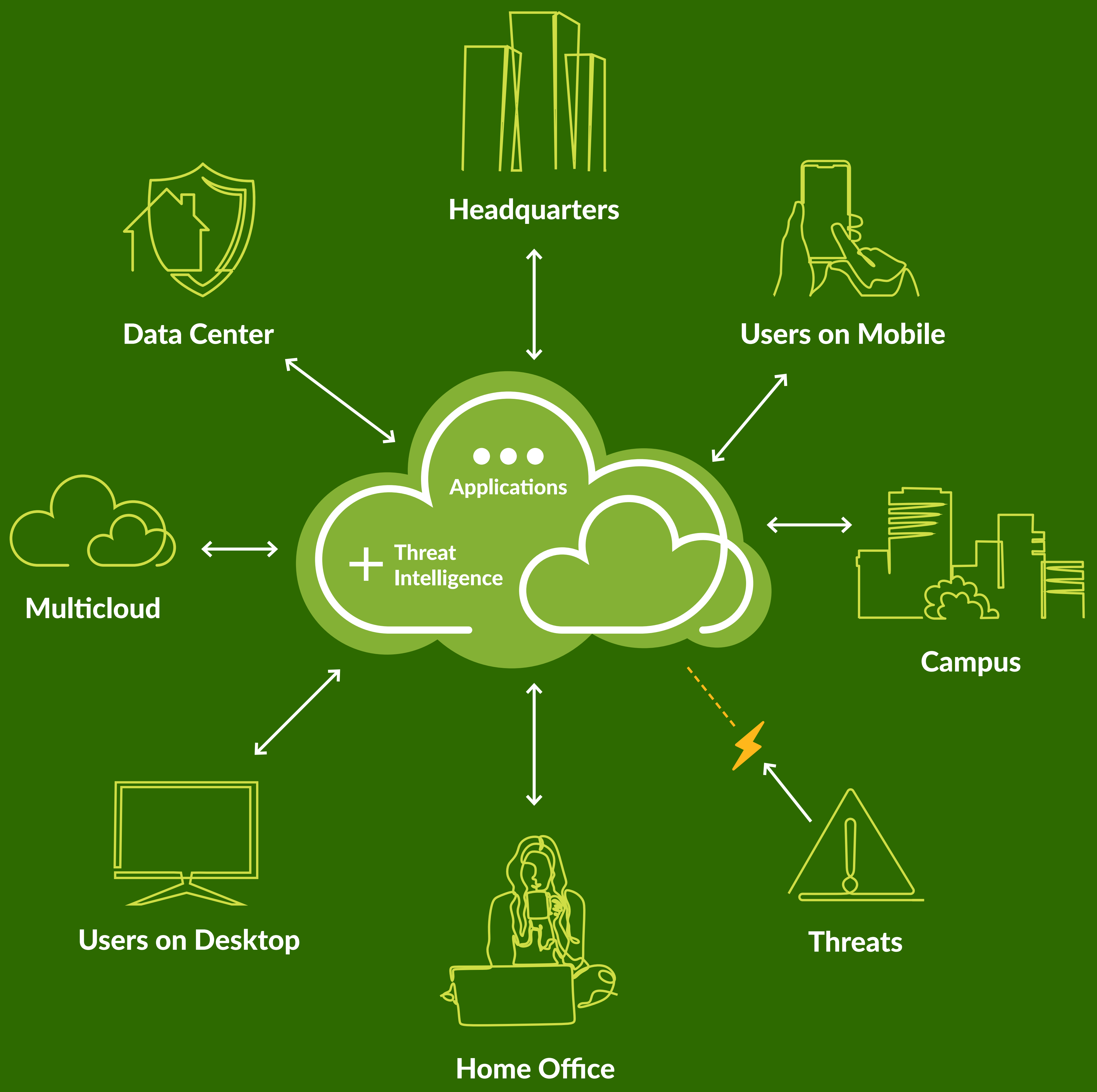
Corporate data will likely be stored in multiple places. It is crucial to take inventory and look at the data holistically.

How is the data being protected in transit and at rest?

Ensure that the data is secure. In what ways is the data being protected? Think about the policies and procedures that are currently in place. Are they consistent across the entire environment? Just the edge? Is data encrypted? Who/what has access to it, and how is it segmented?

Is visibility centralized? What about policy control?

Think about how the network is protected. Is there a clear line of sight into who and what is on the network? How, when, and where are they connecting, and to what? Visibility rarely extends to all corners of the network. How does the organization currently respond to threats? How is access authorized? How is noncompliance handled? Does the entire network get the same attention, or is attention focused on the edge or on a particular public cloud environment?



What current open projects does the organization have? Where is the team challenged or inefficient in its workflows? What areas need to be improved?

Think about the IT team's current open projects and whether those projects will accommodate cloud-hosted services in the next two to four years. What considerations should be taken into account about the existing architecture in order to prepare? Where is the dev repository? Are the backup services onsite or cloud-based? What other impactful services may move from being local to cloud, or, as we've seen in the last few quarters, certain highly sensitive services moved back on premises?

How is data being segmented throughout the data center and across multiple public clouds?

What happens if something gets past security inspection at the edge? The most sensitive data lives in the data center. It is essential to have visibility throughout the environment, not just at the edge, so the data stays protected.

What does the data flow look like? How is the data planned to move?

Look at how data currently flows in the organization's on-premises deployment. Is it working smoothly? Should changes be made? It is important to have a fully formed plan identifying how the data should move to ensure its integrity across environments.

How to Approach SASE

No two cloud journeys are the same. We all have different regulatory requirements, risk tolerance, security needs, and business demands.

With that in mind, there is no single SASE silver bullet that will solve all of the business challenges an organization faces. We recommend starting by thinking about what is currently deployed.

- **What isn't working?**
- **What gaps exist on the network today that need to be addressed?**
- **What are the inefficiencies within the current deployment?**
- **What elements are frustrating?**
- **What is prompting this transition?**
- **What advantages can SASE provide the business?**
- **What are the biggest challenges?**

It’s okay if you don’t have answers to all of these questions right now. But it is essential to think about the vital tenets that are part of every robust security strategy, no matter where the organization is on its journey to the cloud. These include:

- ✓ Safeguarding users, applications, and infrastructure.
- ✓ Ensuring secure connectivity from client to cloud.
- ✓ Enabling a threat-aware network by extending visibility, intelligence, and enforcement to every point of connection on the network.
- ✓ Applying consistent security policies through centralized management and analytics that curate and apply threat intelligence from different sources.
- ✓ Operationalizing what you see, what you know, and what you do.

Conclusion

SASE is not a cure-all, and by no means is this transition going to happen overnight. SASE is about how the organization chooses to design, build, and maintain the network architecture to optimize user experience and secure services and data.

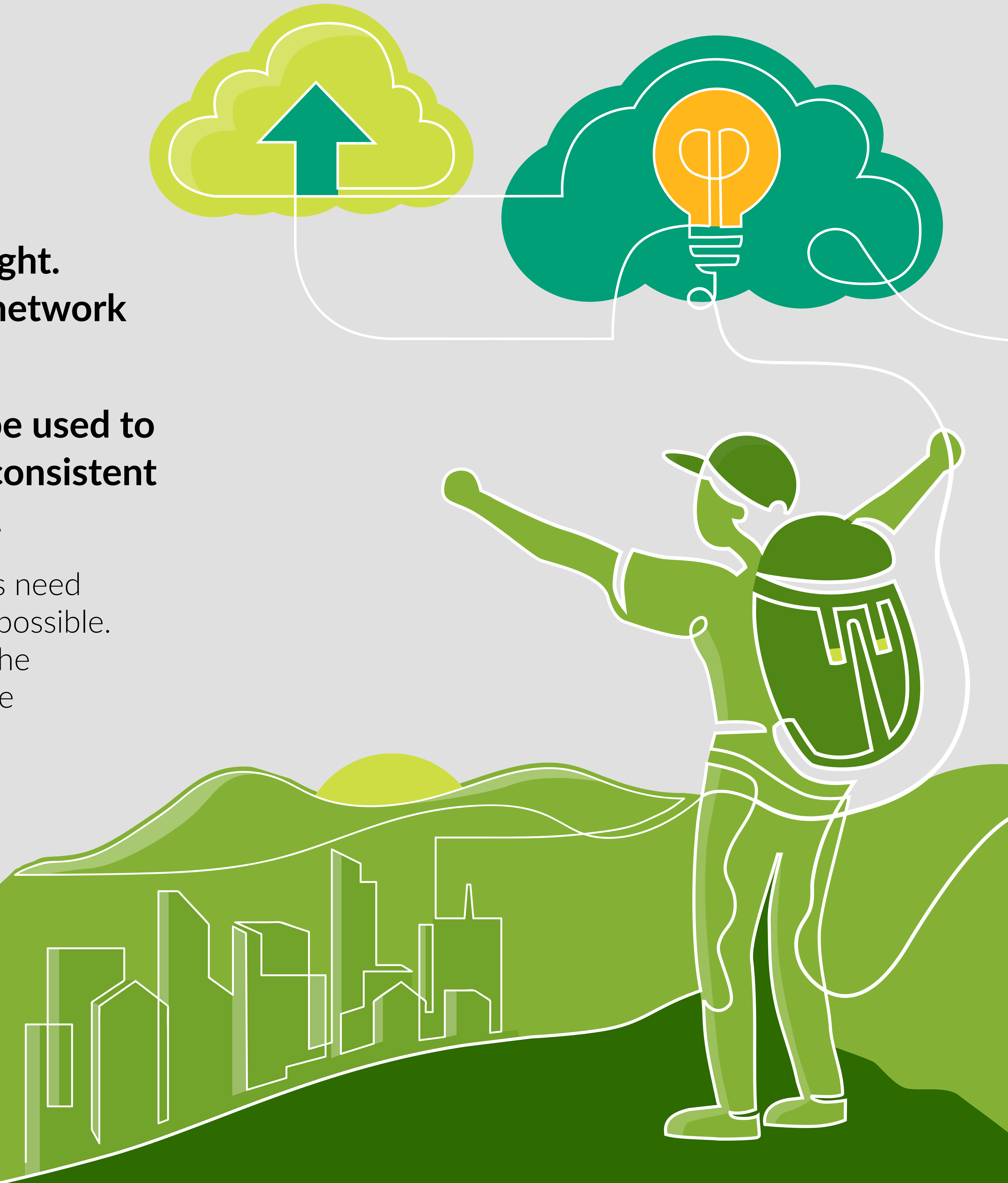
Threats can be introduced into the network from many sources, and SASE can be used to protect against these attacks, regardless of where the user is located, ensuring consistent security enforcement without having to backhaul traffic to a corporate location.

It is important to understand which elements of SASE exist on the network already and which gaps need to be addressed first. Also, consider what dedicated resources are required to make this transition possible. The best network can accommodate both cloud and on-premises infrastructure while supporting the transition and the ongoing needs of the business. Every organization needs a diverse and adaptable architecture to support business now, and in the future.

Learn more about SASE

Read our blogs:
The Road to SASE is a Journey, Not a Sprint
Next Stop on the SASE Journey: Establishing a Plan and Team for Success
Architectural Choice: The Key to a Successful SASE Journey

Listen to our Podcast:
What is SASE?



JUNIPER NETWORKS

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

PN: 7400131-001-EN