CATO
NETWORKS

5 Questions to Ask Your SASE Provider

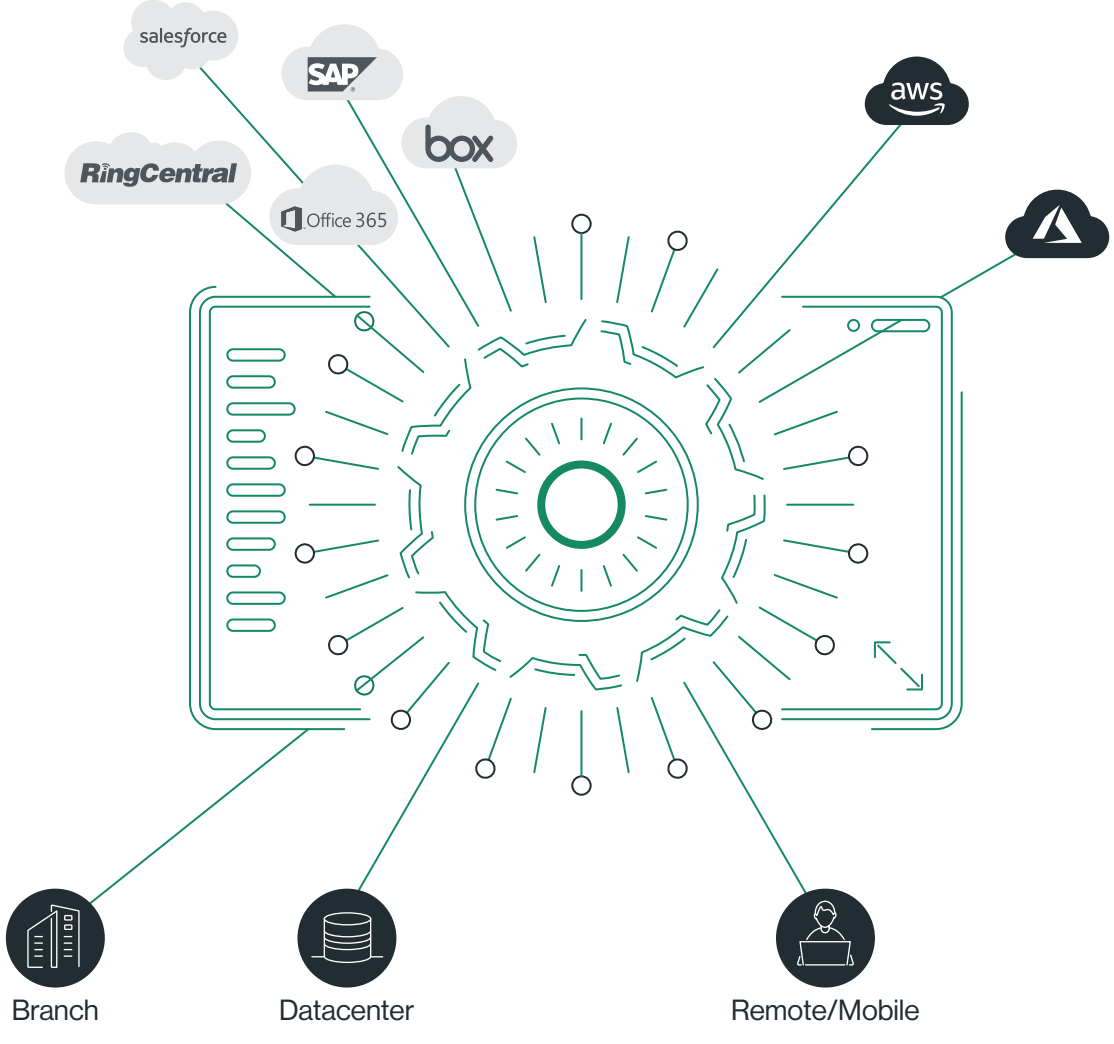
Secure Access Service Edge or SASE is a term that describes the convergence of enterprise networking and security capabilities delivered at global scale as a cloud delivered service. Since Gartner coined this term in 2019, many vendors have been quick to jump onboard.

Despite many labeling themselves and their products as SASE, there is quite a bit of disparity between each vendor's capabilities and architecture. Ask your prospective SASE vendors these 5 questions to evaluate how well their architecture aligns with the SASE vision and if their capabilities will position your organization for success into the future.

1/ Do you provide complete visibility and control for all traffic and all edges (users, branches, data centers, cloud)?

While this question sounds simple and straightforward, it is multi-faceted, and you should carefully evaluate the response from your prospective vendor. Support for all edges is a key tenant of SASE, yet not all vendors treat all edges equally.

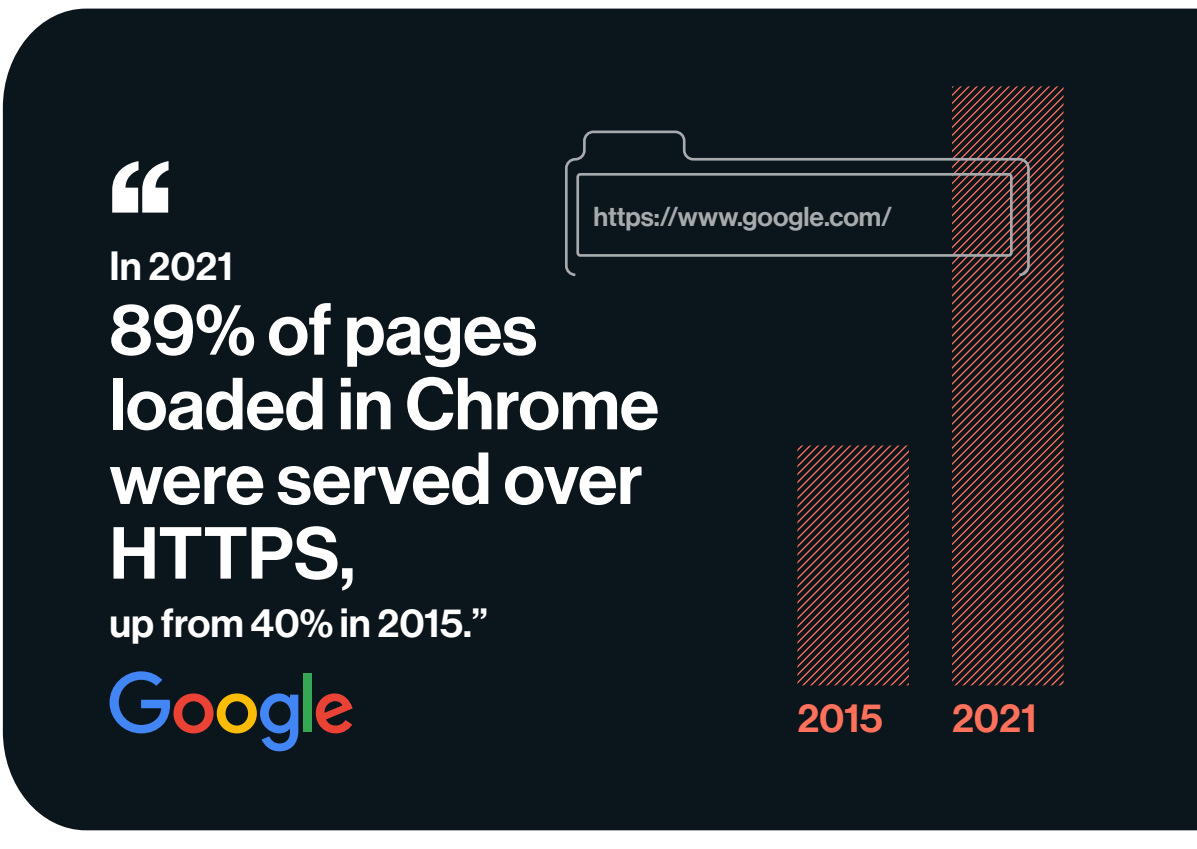
Your SASE solution should allow **full mesh connectivity between users, locations, and cloud resources**. Some solutions may apply access and security separately, leaving capability gaps that require the purchase, implementation, and maintenance of additional products to meet your needs.



Beyond the need to **support all edges**, an effective SASE provider should also support all traffic. This means support for network segmentation, WAN, and Internet traffic as well as active inspection of all ports and protocols. Some vendors have architectural limitations that prevent them from delivering value in all the above areas.

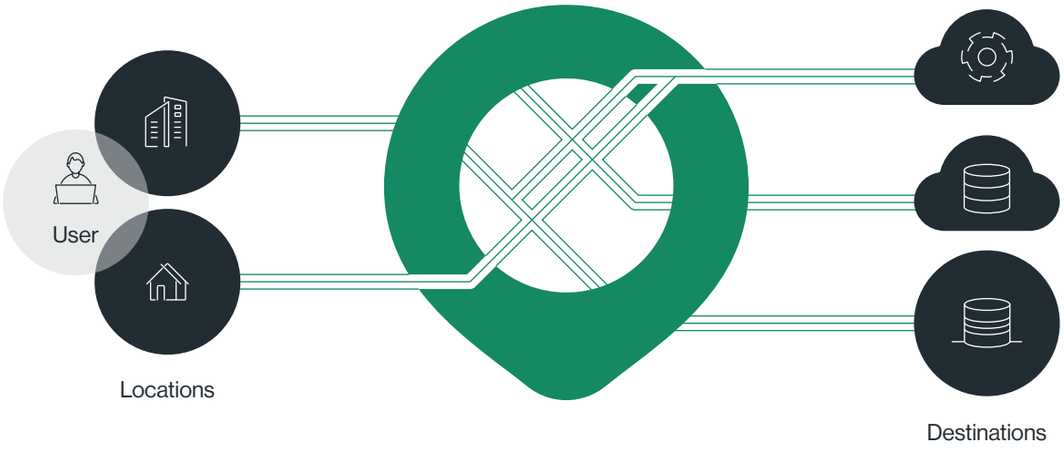
For example, a solution built around a web-proxy architecture may be able to ingest traffic from all ports and protocols, and even offer basic NGFW access control capabilities, but can only provide inspection for a select number of protocols. All traffic, whether north/south or east/west should be inspected for malware and data exfiltration. This single platform approach reduces security gaps and enables complete visibility and control.

Finally, your chosen vendor should allow you to **enable TLS inspection at scale** without performance impacts. In 2021, 98% of Google's page one results are HTTPS. This means that if you are not performing TLS inspection, you have blind spots that leave you vulnerable. Not only should inspection be easy to enable, granular controls should also be provided allowing you to exclude categories (finance, health), hosts and users as necessary.



2/ Does your solution allow users to seamlessly transition from corporate offices to other locations and back?

The SASE approach enables providing always-on security and access to users at any time and any location. Because of this, effective solutions natively transition between office and other networks, without any interaction from the user. This means that the agent on the user's endpoint should detect corporate networks and behave appropriately when connected or disconnected from them. No third-party products or integrations should be required for this.



In addition to providing users with seamless roaming between various locations, a SASE provider will ideally provide individual mobile users with the same capabilities as when they are in the office. Security and remote access are typically the focus, but you shouldn't forget to consider performance and optimization.

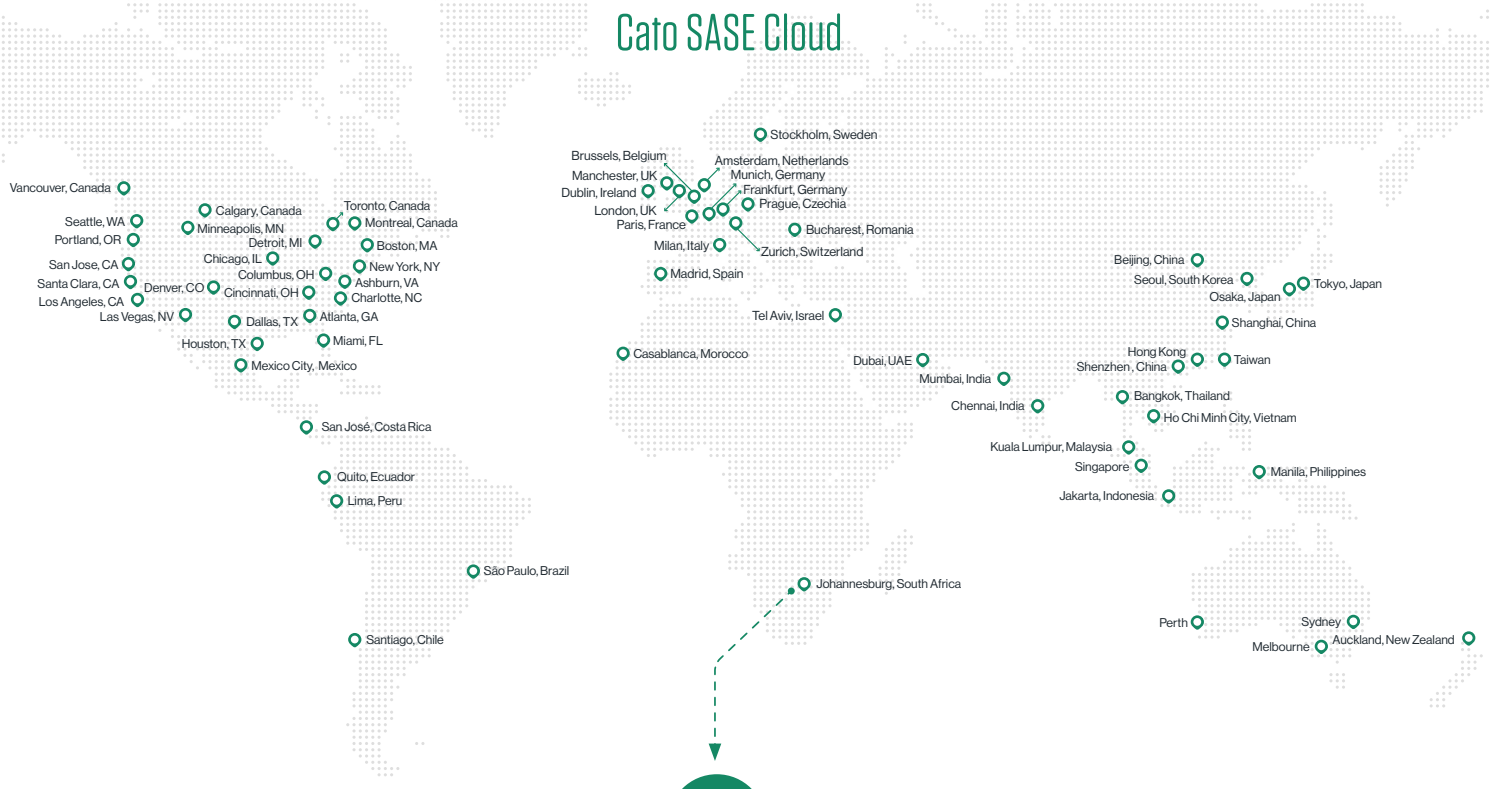
After all, one of the qualities of SASE and its global presence is to improve the user experience. Since SASE is the convergence of networking and security, SASE vendors should be able to apply QoS, optimization and other networking policies to mobile users, not just branch offices.

> **"After Covid-19, 82% of respondents indicated that their companies will continue with work from-anywhere or remote only models."**
>
> CATO NETWORKS

3/ What is the global presence of your service?

It's unfortunate, but frequently the number of PoPs advertised by a SASE provider is misleading. In some cases, the vendor is counting logically separated hardware that sits in the same rack as one of their "other PoPs," and delivers no additional value to customers. For SASE providers that rely on public cloud infrastructure, the number advertised is likely inflated through the inclusion of "on-ramp" locations that backhaul traffic to a small number of compute locations where security is applied.

Regardless, you should understand which unique geographic locations will be accessible to your organization, how your traffic will be handled, and whether to expect performance impacts that may result from the providers architecture. Once you have this information, you can compare it to the current and future needs of your company.



Dynamic Flow Orchestration

- Any customer, any edge
- Contextual policy enforcement
- Dynamic load balancing
- Cloud-scale
- Self-healing
- Self-maintaining

NETWORK

- Edge SD-WAN
- WAN Optimization
- Global Private Network
- SAAS Optimization
- Multi-Cloud Networking

SECURITY

- Next Generation Firewall
- Secure Web Gateway
- Next Generation Anti Malware
- Intrusion Prevention System
- Cloud Access Security Broker
- Data Loss Prevention
- Remote Browser Isolation

Beyond understanding the global footprint of your SASE provider, it is important to discuss the delivery of features and capabilities in relation to PoPs. Many vendors were short sighted when developing their architectures and cannot deliver all capabilities at every location. A true SASE provider should be able to deliver security and access as a converged service from every PoP location, traffic should not have to be sent to another PoP for a malware or DLP verdict.

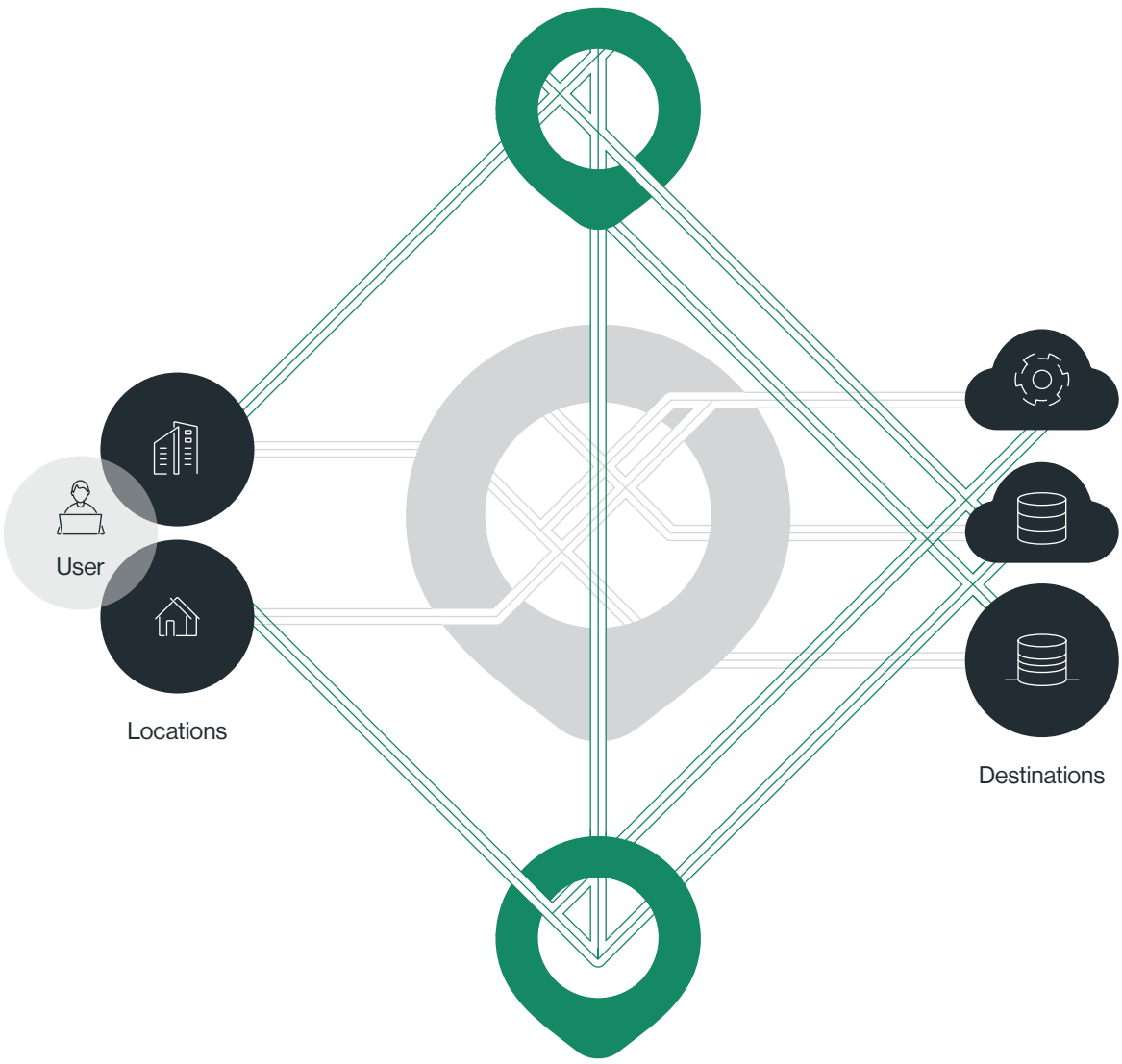
You can also ask your provider if they utilize a private backbone, not just for orchestration and management of the service, but for the performance and optimization of your traffic. While a private backbone isn't necessarily a key component of SASE, when you consider the global scale of the service, it makes sense. A vendor that is utilizing a global private backbone can provide better performance to your users with lower costs to your organization.

You should be able to create policies to optimize traffic across the backbone, not just between your locations, but to SaaS and public clouds as well.

4/ Is your service architected for resiliency and self-healing?

When you make SASE your network, an outage can be catastrophic to both profit and productivity. When all your employees' access is at stake, you want to know that your SASE vendor has your back. High availability (HA) can be divided into two areas, service level and site level.

The service level has to do with your vendor's infrastructure and orchestration. Most vendors will claim that their service is fully resilient, but you should ask the right questions to ensure that their resiliency model aligns with your expectations. For example, while most vendors have built intra-PoP failover, many leave inter-PoP failover up to their customers. Ask your vendor if they have ever requested a customer to failover to another PoP location, or if they provide a solution for this. Ideally failover of any kind should be transparent to and have minimal impact on users.



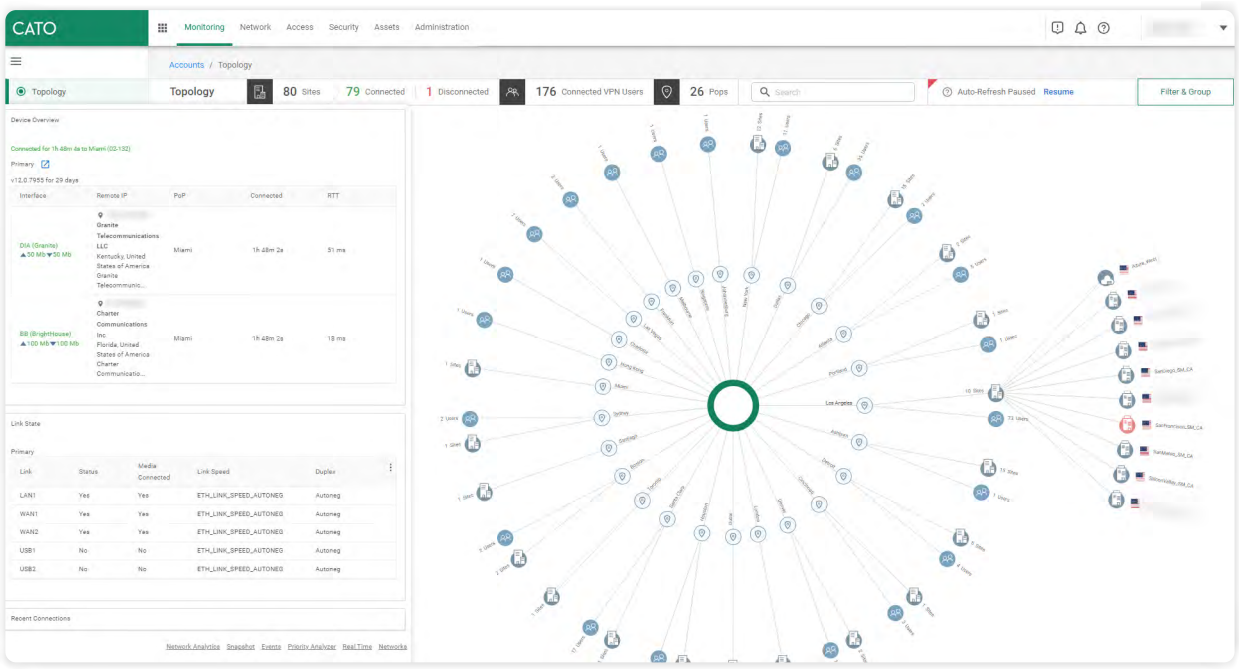
Site level failover has to do with the equipment at your locations and their connectivity to your SASE provider. This can relate to redundancy of equipment or anything else that relates to connectivity. Some SASE vendors only provide you with the ability to create multiple IPSEC tunnels, leaving it up to you to architect your HA connection to your provider. Depending on your vendor this may be ineffective, difficult, or expensive.

Check with your prospective SASE vendors to ensure they have a simple solution for providing HA at your locations.

5/ Can all aspects of your solution be accessed and managed from a single management application?

A good way to ensure that the SASE solution you are considering is well architected and focused on simplicity, is to look at the number of applications required for managing it. If a vendor has separate products for security and remote access, there may also be separate management applications, configurations, and policy sets. This means that the products are not unified on the backend and likely were not architected as part of a single platform.

The utilization of separate consoles creates additional complexity and increases the probability of misconfigurations and security gaps. Additionally, logging information is not unified, making it difficult to troubleshoot issues or investigate suspicious activity. Exporting both log sets to a SIEM is the only solution, adding more cost and complexity.



Beyond having separate consoles, some vendors may have a robust management application that manages multiple products in their portfolio. This sounds like a great idea until you must use the application and find that it is bloated and dependent on plugins. Not only do you have to host this application yourself, but you now must ensure you have staff with relevant expertise, as well.

This is great for your vendor as it locks you in, but not always so great for you or your organization. Furthermore, such a legacy management application can be a barrier to innovation and may link you to web-based consoles to use newer features. There may be a new option from your vendor, but make sure it has feature parity before you go down that route.

Lastly, don't forget that managing the SASE service from your vendor may not be the only thing you have to think about. While true SASE vendors converge networking and security, others cover only parts of the picture. You may have to manage SD-WAN or other devices used for IPSEC connectivity using separate consoles.

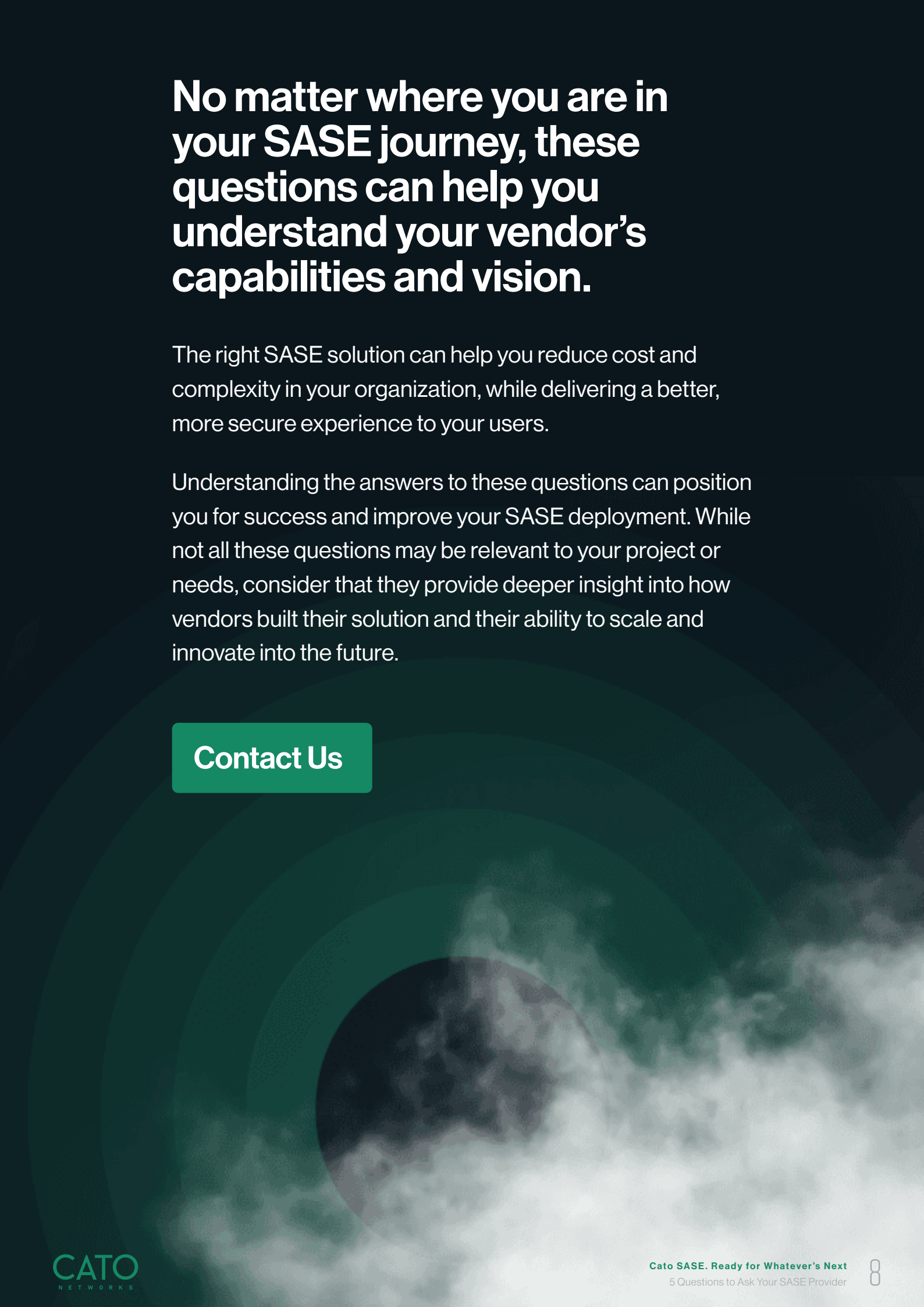
More consoles not only create more complexity and increase troubleshooting times, but may also indicate a service that isn't fully converged or cloud-native.

No matter where you are in your SASE journey, these questions can help you understand your vendor's capabilities and vision.

The right SASE solution can help you reduce cost and complexity in your organization, while delivering a better, more secure experience to your users.

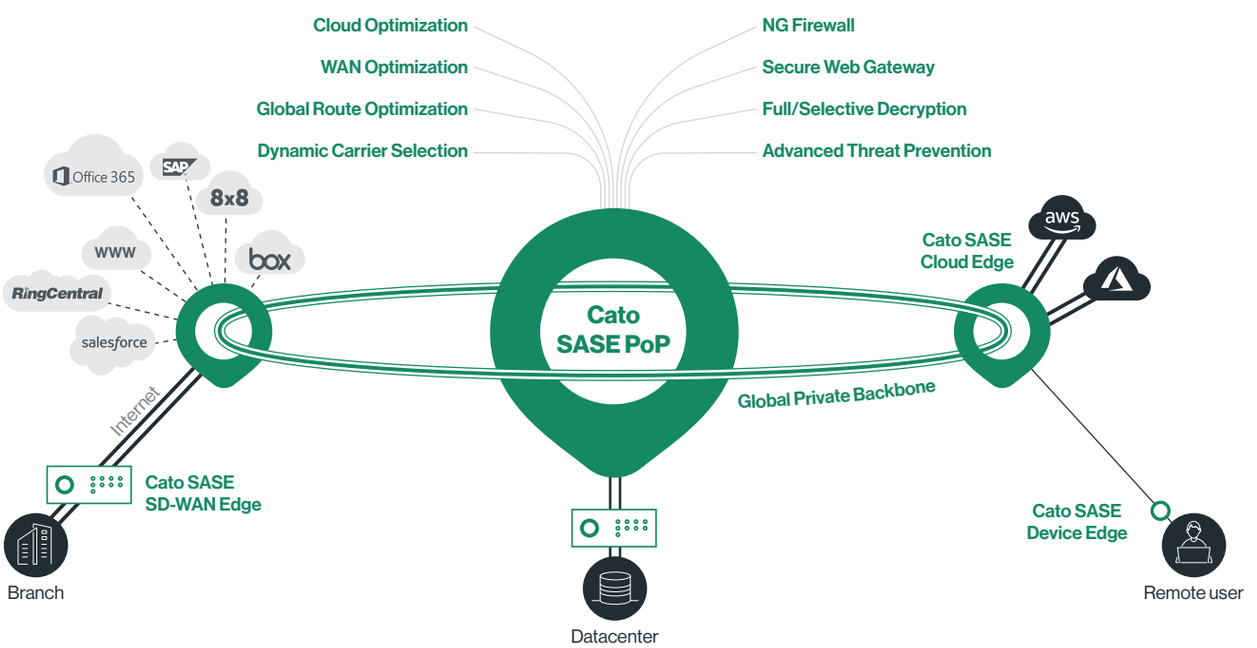
Understanding the answers to these questions can position you for success and improve your SASE deployment. While not all these questions may be relevant to your project or needs, consider that they provide deeper insight into how vendors built their solution and their ability to scale and innovate into the future.

Contact Us



About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato SASE Cloud, customers easily migrate from MPLS to SD-WAN, improve connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud data centers and remote users into the network with a zero-trust architecture. With Cato, your network and business are ready for whatever's next.



Cato SASE. Ready for Whatever's Next

Cato SASE Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Secure Remote Access
- Unified Management Application

Use Cases

- MPLS migration to SD-WAN
- Optimized Global Connectivity
- Secure Branch Internet Access
- Cloud Acceleration and Control
- Remote Access Security and Optimization
- Flexible Management

SOC2 Approved | ISO 27001 Certified | GDPR Compliant | Gartner peerinsights Customer first

CATO NETWORKS

Contact Us

Useful Links

eBook

What to expect when you're expecting... SASE

eBook

SASE for Dummies 2nd Edition is Now Available!

eBook

Ransomware is on the Rise – Cato's Security as a Service can help

eBook

The ROI of Doing Nothing

Whitepaper

SASE: Networking and Security Architecture for the post COVID-19 World

Whitepaper

Have it the Old Way or Enjoy the SASE Way