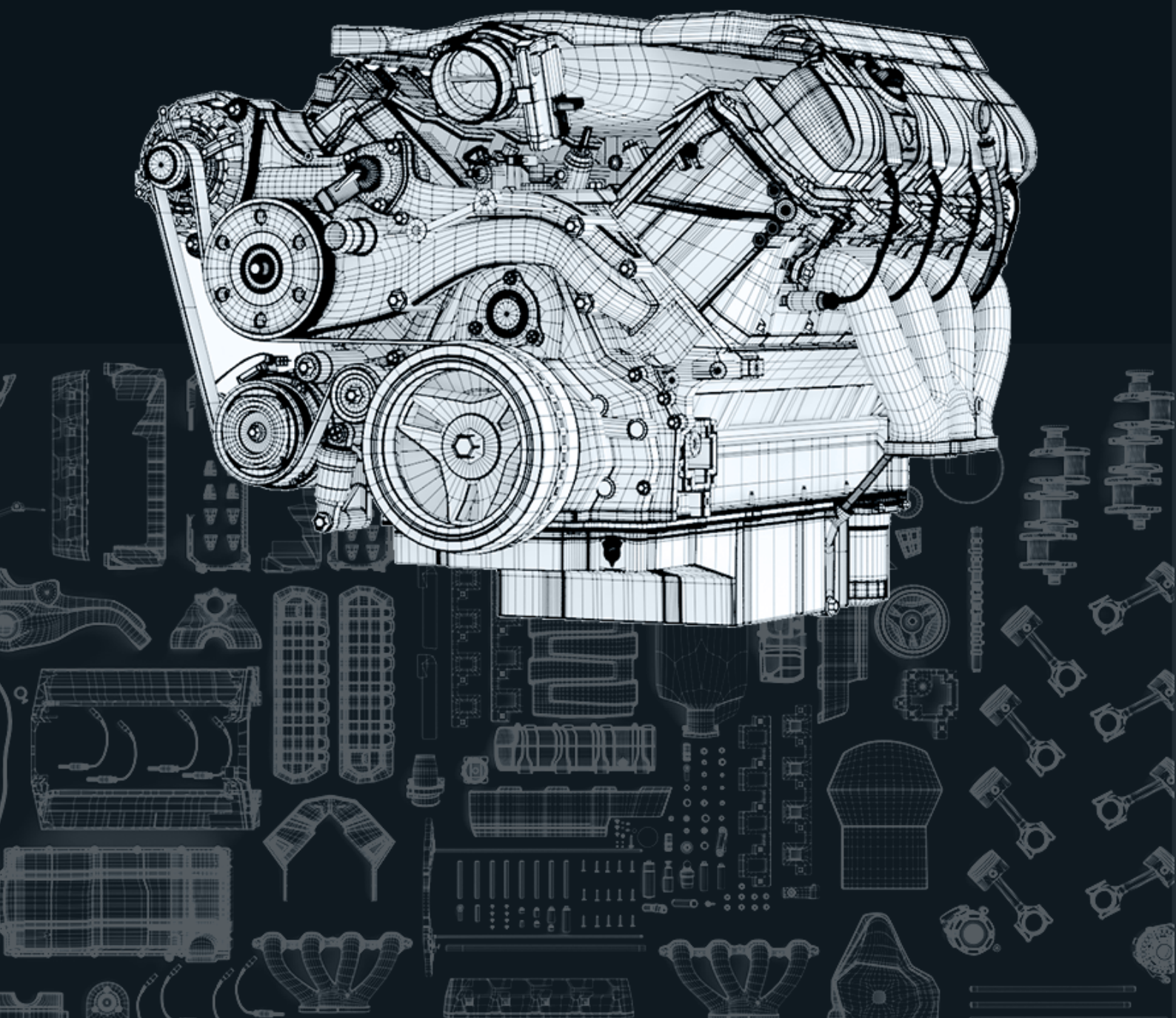
CATO NETWORKS

Achieving Better Security

Convergence vs. Sum of Parts



What is SASE

Secure Access Service Edge or SASE is a term Gartner coined in 2019, representing the convergence of networking and security into cloud-native service offerings. Gartner analysts claimed that the legacy "data center as the center of the universe" architecture is obsolete, inhibiting the needs of modern organizations due to complexity, lack of scale, and poor performance (especially evident during COVID-19). This was due to several factors, primarily the increasing mobility of users and the migration of applications from the corporate data center to the cloud.

This concept turns the traditional security and networking model upside down. Rather than backhauling traffic from users and locations to a central data center for inspection and policy application, security is brought to the user. SASE allows organizations to deliver security and access on a global scale, strengthening the organization's security posture while creating a high-performance experience for users and enabling cloud transformation.

While there is still some debate regarding which capabilities are essential to SASE, Gartner makes it clear that an identity-centric cloud-native architecture that supports all edges (mobile user, site, data center, cloud data center) is essential. Some of the capabilities recommended by Gartner as being potential SASE components include SD-WAN, WAN Optimization, CASB, SWG, ZTNA, FWaaS, DNS, and RBI, among others. Few vendors offer a holistic approach to SASE, often relying on loose integrations of disparate products and partnerships with other vendors; typically, they are established vendors with legacy products they attempt to position as SASE offerings.

Integrated Solutions – The Legacy Approach

SASE is still relatively new and includes a variety of offerings traditionally sold as point solutions from various vendors. It is easy to understand why legacy vendors rely on integration to deliver what they label as a comprehensive solution. The fastest way to enter the SASE space for most vendors is to modify and deploy an existing product into public cloud providers such as Azure, AWS, or GCP. Then, utilizing multiple integrations, this product is enhanced by partnerships or acquisitions to include additional features outside of the scope of the original "best of breed" product. This can include SD-WAN, RBI, and even WAN optimization and global connectivity. This approach is logical given the circumstances but is not without drawbacks. Even vendors who do not utilize public cloud providers for service delivery can have limitations based on how they architected their solution and their reliance on integrations with third-party products to fill in gaps.

Integrated SASE offerings cannot deliver on the value promised by SASE due to:

Increased Complexity

SASE aims to reduce complexity and enhance the scalability of security and access offerings globally. Integrated solutions typically still require multiple management consoles or the purchasing of a stand-alone management solution. This can increase costs but more importantly, adds additional management layers and reduces organizational agility when deploying, maintaining, or troubleshooting the product(s). Also, the offering may rely on multiple integrations that may be poorly developed, leading to outages, security gaps, or a failure to deliver the desired capabilities. Often, these integrations require a high level of effort from the customer and do not provide immediate functionality. In some extreme cases, customers may need to build their integrations to achieve the desired outcomes.

Poor Performance

Architecture is a critical factor in delivering SASE as a high-performance service. Single Pass Processing or some variation of this terminology is a buzzword in SASE but consider that not all single-pass promises are genuine. Single-pass implies that all engines are acting simultaneously to process traffic flows for access control, optimization, threat, and data protection, minimizing processing latency. If a solution relies on integrations for security, SD-WAN, global connectivity, or other functions, the vendor isn't delivering an authentic single-pass architecture. Instead, service chaining must be used to hand off flows between the various engines, and the single-pass designation is just marketing that only applies to part of the solution. This adds processing latency, sometimes even sending data to other PoPs for things like DLP or zero-day analysis.

Limited Vendor Control

When decisions are made to leverage the public cloud, integrate with a partner, or integrate an acquired solution, the vendor loses some control over the functionality and delivery of their SASE platform. While it is not always prudent to develop every component in-house, the advantages to customers of this approach often outweigh the disadvantages. A few examples of this include clumsy "zero-touch" provisioning requiring a plug-in or using internet-published JSON or XML lists for tunnel creation from SD-WAN appliances. Both methods certainly ease deployment to some extent but still need a significant amount of manual effort on the part of administrators. Another example relates to PoP expansion; some vendors are limited by their public cloud providers' presence or architecture and have difficulty scaling their solutions to new geographic regions. Beware that some vendors will exaggerate their PoP count by including on-ramp locations that backhaul traffic to a small set of compute PoPs or even counting hardware deployed to the same data center as multiple PoPs. When considering a vendor, always determine which unique geographic locations will be accessible to you in deployment and at what cost.

Increased Opportunity for Security Gaps

This problem ties back to the increased complexity of managing integrated solutions but also goes all the way back to the architecture of legacy solutions. The more products and integrations introduced the greater chance for failure. This can be due to the integration itself or from policy sprawl, multiple policies across multiple products, and management consoles that create inconsistencies and leave room for misconfigurations or unintended results. Furthermore, legacy solutions are a byproduct of the evolution of security technology, this is evident in the creation and assignment of customizable security profiles to various policies. Some may find this level of control to be a benefit, but more often it results in inconsistent application of security inspection engines.

Lack of Full Visibility

Integrated SASE offerings are intended to present a complete solution to customers, but often still rely on multiple management consoles and data sources. Networking and security log data are stored and often accessed separately, making correlation extremely difficult. While vendors will happily sell you additional solutions to aggregate this data, it erodes the value of SASE by reducing the context available to security engines when making verdicts on traffic.

> **"Convergence of security systems must produce efficiencies that are greater than the sum of their individual components."**
>
> Gartner | Infrastructure Security Primer for 2022

Convergence – The Measure of True SASE

As discussed, SASE takes existing capabilities and transforms them into cloud-native services. The primary difference between a converged offering and an integrated one is that the former was built from the ground up to deliver both security and networking capabilities while the latter is pieced together from existing products. Convergence can be challenging because it takes time to build a new platform from the ground up. So, it is easy to see why legacy vendors choose an integration approach to get to market faster.

This means that integrated solutions benefit the vendor more than the customer, and the differences are clear when you consider these areas:

Rapid Deployment

Deployment speed will vary from organization to organization, but you should consider if a solution is helping or hurting in this area. For example, an integrated solution may require configuration in multiple consoles, manual deployment of IPSEC tunnels, purchase, deployment, and hosting of a management application, sizing, and deployment of virtual machines, or even waiting for resources to be provisioned in desired geographic location. Each of these factors can dramatically increase deployment time and the complexity of the overall solution. Remember that the complexities of deployment also bleed over into maintenance and management of the solution over time.

Single Management Application

"Single pane of glass" management is an overused term by many vendors but is often misleading. For some, it may mean a primary management application or console that you own and install plugins on to manage different solution components, or it can be web-hosted but link administrators to other applications that are required for specific features. Overall, a real single point of management decreases administrative overhead and allows for simplified investigation and troubleshooting.

True Single-Pass Processing

Another overused industry term, almost every vendor has their own acronym to represent this as part of their architecture. Essentially it represents a decrease in processing latency due to simultaneous inspection/policy application on traffic by multiple engines. While this may be true for individual products, remember that integrated solutions cannot have this apply holistically, but rather require service chaining to some extent as traffic is handed off between capabilities, effectively separating networking and security functionality and introducing latency.

Cloud-Native, Not Cloud Delivered

Cloud-native solutions are purpose-built to deliver scale, flexibility, and resilience and are not quite the same as "cloud-delivered." Cloud-delivered refers to hosting virtual machines in a public cloud provider such as AWS, GCP, or Azure. The cloud-delivered approach aligns with the need of legacy vendors to quickly deliver a SASE offering based on their existing product capabilities. A genuine cloud-native solution will be multi-tenant and hosted in top-tier data centers globally. Keep in mind that integrated solutions may have some components that are cloud-native, but others that are cloud-hosted. Cloud-native architecture provides the vendor with more control over the solution and enables better capabilities and performance in more locations.

No Hybrid or On-Premises "SASE" Deployments

As a rule, organizations should be wary of any vendor that offers a hybrid or on-premises SASE deployment. SASE by nature requires that the service be delivered from a cloud-native platform. While a hybrid deployment may be appealing to those who are early in their cloud journey, please consider that this is an indication of a vendor that wants to gain traction with SASE but doesn't have a real SASE product. Instead, they are merely relying on integrations and appliances to deliver capabilities that should be offered with the global presence and infinite scale of the cloud.

Not to over-simplify, but here is a simple anecdote to explain the difference between integrated and converged. An integrated solution is a bit like an independent mechanic building you a car from old parts found around the repair shop. A converged solution is like purchasing a brand-new car. Both can effectively accomplish the same thing to some extent, but one is pieced together and full of compromises while the other has all parts working together as designed.

> **One vendor had an excellent infrastructure, but very limited security, so we would have had to go to another vendor for content filtering, just like with our current solution. Another vendor relied to a large extent on its endpoint security appliances, so it wouldn't relieve the complexity of our current appliance-based architecture."**
>
> 
> Alexander Azikov, IT Manager at Diamond Braces

Integrated or Converged – What to Look For:

As discussed, SASE takes existing capabilities and transforms them into cloud-native services. The primary difference between a converged offering and an integrated one is that the former was built from the ground up to deliver both security and networking capabilities while the latter is pieced together from existing products. Convergence can be challenging because it takes time to build a new platform from the ground up. So, it is easy to see why legacy vendors choose an integration approach to get to market faster.

This means that integrated solutions benefit the vendor more than the customer, and the differences are clear when you consider these areas:

	Integrated	Converged
Native SD-WAN Available		×
SD-WAN from Partners	×	
Single Management Application		×
Multiple Management Consoles	×	
Full Mesh Connectivity		×
Requires VM Deployment	×	
Requires Tunnel Configuration	×	
Optional Use of IPSEC Tunnels		×
Hosted in Public Cloud	×	
Separate Authentication Flows for Security & Access	×	
Requires SIEM for Correlation of Network & Security Events	×	
Optional Export to SIEM		×
Hybrid Deployment	×	
Separate Networking, Security, and Remote Access Products	×	
Multiple Products Required	×	
Different Capabilities for different PoPs	×	
All PoPs fully Capable		×
Consistent Policy Enforcement		×

Integration is a Vendor Sales Strategy, not a True Benefit of SASE

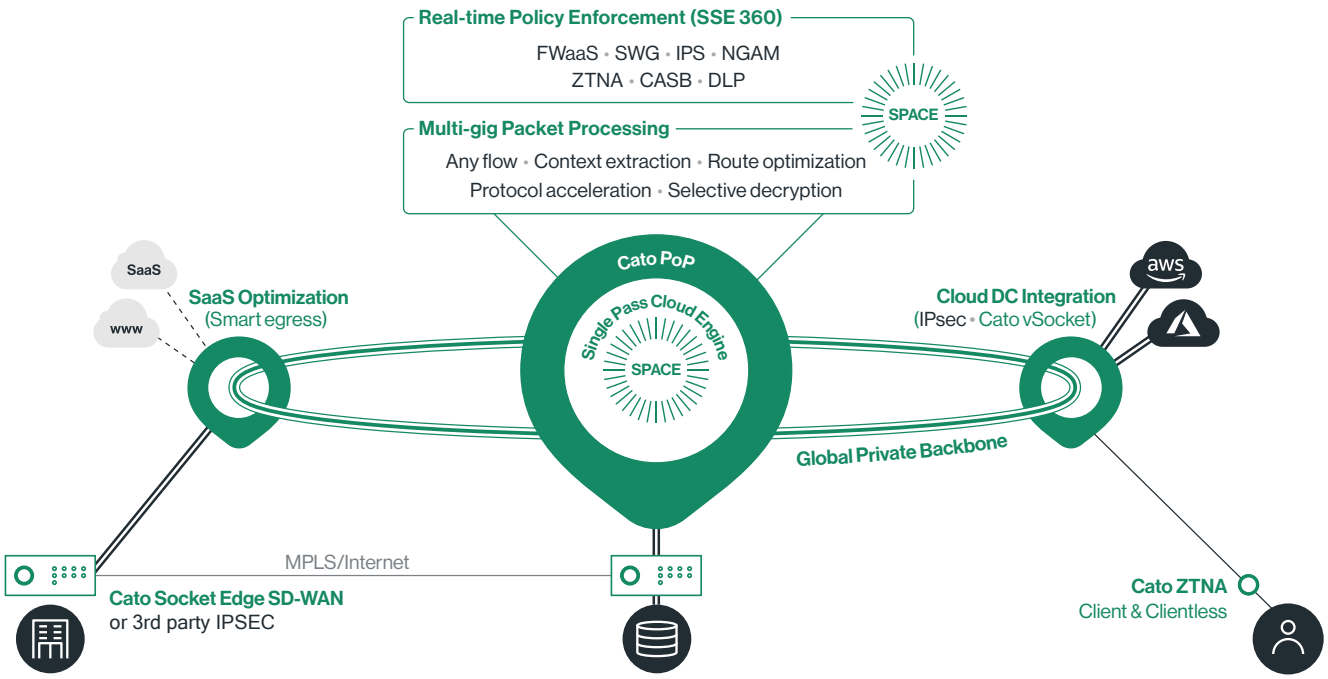
Integration is an approach favored by legacy vendors to allow them quicker entry into the SASE market. These companies have significant investments in their existing “best of breed” point products and hardware. This approach erodes the value of SASE by creating additional complexity for administrators and a poor user experience. Convergence is the future of security and networking, allowing seamless delivery of all capabilities from a single cloud-native platform on a global scale.

When evaluating SASE providers consider the advantages of a converged platform for your current and future needs across multiple use cases. This includes eliminating or reducing MPLS, replacing legacy VPNs, enabling cloud adoption, securing branch internet access, and securing mobile users. Finally, ensure the solution (converged or not) is future-proof, allowing you to quickly adopt new functionality as it becomes available.

About Cato Networks

Cato provides the world's most robust single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Cloud optimizes and secures application access for all users and locations everywhere. Using Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration.

Cato SASE Cloud with SSE 360



Cato SASE Cloud

- SSE 360
- Secure Remote Access
- Edge SD-WAN
- Global Private Backbone
- Multi-cloud / Hybrid-cloud
- SaaS Optimization
- Cato Management Application

Use Cases

- MPLS Migration to SD-WAN
- Secure Remote Access
- Secure Branch Internet Access
- Optimized Global Connectivity
- Secure Hybrid-cloud and Multi-cloud
- Work From Home

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.