FORTINET

COMCAST BUSINESS

The 8 Critical Security and Networking Challenges Every SASE Strategy Must Solve

Table of Contents

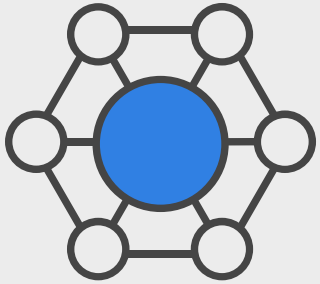
Executive Summary

Employees connect from offices, homes, branches, and everywhere in between, accessing applications that live across data centers, public clouds, and Software-as-a-Service (SaaS) platforms. The challenge for IT and security leaders is consistent: deliver a fast, frictionless user experience while enforcing enterprise-grade security on every connection, no matter where the user or application sits.

By converging networking and security into a single, cloud-delivered service, secure access service edge (SASE) replaces the complexity of legacy VPNs, point security products, and rigid hub-and-spoke designs with a unified architecture that follows the user.

Selecting the right SASE partner can ensure operational success. The wrong partner may have you struggling just to keep all of your organization's essential elements working together. Many SASE vendors entered the market quickly, often with immature security stacks, isolated point products, and limited use case coverage, adding to vendor sprawl instead of reducing it.

This ebook was created to help you evaluate SASE offerings. It covers the signals shaping SASE demands, the eight use cases your solution must address, and what makes the Fortinet and Comcast Business managed SASE solution stand out.



“Organizations require solutions to be deployed at the speed of their business, with the flexibility to meet them where they are in their SASE journey, not requiring a rip-and-replace as the only option.”

–Rick Mashburn, VP Systems Engineering, Fortinet

Introduction

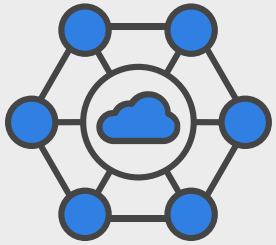
This ebook captures insights from a strategic roundtable discussion featuring experts from Fortinet and Comcast Business. Together, we explored the evolving state of SASE (secure service edge [SSE] plus SD-WAN), the growing expectations customers have for managed security services, and the critical factors organizations should evaluate when selecting a managed SASE provider. Read on for practical guidance on navigating the next phase of secure connectivity.

The Fortinet and Comcast Business partnership brings together two industry leaders with complementary strengths. Comcast Business has a nationwide IP network, managed services leadership, and enterprise-scale delivery. Fortinet delivers global cybersecurity innovation, AI-driven threat intelligence, and high-performance security platforms.

Expectations for Today's SASE Solutions

Across industries, organizations are landing on three key priorities for their SASE solutions:

- **Consistent security with consistent user experience:** Users need to be protected wherever they work, but not at the cost of latency or friction. SASE consolidates security functions into a single service, so policy follows the user instead of being trapped at the network edge.
- **A move from VPN to zero-trust network access (ZTNA):** Traditional VPNs grant implicit, broad-network access once a user is authenticated. Modern enterprises require explicit, per-application access that is verified continuously through device posture checks. SASE provides the architecture for that shift.
- **Operational simplicity through unification:** Multivendor SASE deployments add complexity when simplified solutions are what's needed. Organizations are asking for a unified stack of SD-WAN and security services that works out of the box, with AI-driven assistance simplifying network operations center (NOC) and security operations center (SOC) operations.



“Whether an enterprise is in healthcare, banking, or retail, SASE makes sense for many reasons. It could be that they’re trying to move off of a legacy MPLS network, that they’re working with hundreds of different cloud service providers and need to secure their applications, or they could have a mobile workforce with users all over that need to connect securely.”

–Joe Austin, Comcast

The 8 Use Cases Your SASE Solution Must Address

Before evaluating any vendor's offering, map your needs to the use cases SASE was designed to solve. If a provider can't credibly check all eight, gaps will surface later as risk, downtime, or unexpected cost.

1. Secure internet access

Hybrid workers need direct internet access, but every direct path expands the attack surface. Look for SASE that goes well beyond an encrypted tunnel. Integrated technologies should include secure web gateway, URL filtering, DNS security, antiphishing, antivirus, antimalware, sandboxing, and ZTNA. They all must work together to respond to known and unknown threats.

2. Secure private access

Whether your applications live in a private data center or a public cloud, ZTNA should grant explicit, per-application access to authenticated users. The right SASE solution integrates SD-WAN and next-generation firewalls to find the shortest path to those applications, ideally through a single agent that combines traffic redirection, ZTNA, cloud access security broker (CASB), and endpoint protection.

3. Secure SaaS access

With SaaS now a primary work surface, modern SASE must include dual-mode CASB (inline and API-based) to address shadow IT and protect critical data. SaaS security posture management should also be embedded into the platform, automatically detecting and remediating misconfigurations across SaaS applications without forcing you to buy yet another point product.

Another key requirement is the ability to identify unsanctioned cloud usage and enforce real-time policies that govern and control safe generative AI (GenAI) adoption by employees.

4. Cloud-based management with hybrid interoperability

Cloud-delivered visibility, reporting, logging, and analytics shorten mean-time-to-detect and mean-time-to-respond, but only if the SASE management plane interoperates cleanly with on-premises management. Otherwise, you've simply added another console to the IT team's burden.

5. Simplified onboarding and flexible consumption

SASE economics matter as much as SASE technology. Tiered, predictable licensing, paired with simple onboarding, granular reporting, and integrated digital experience monitoring (DEM) for proactive troubleshooting keeps cost aligned to business growth and avoids tying up capital in excess hardware.

6. Protection for microbranches and pop-up locations

Small offices, home offices, and short-term sites need the same protection as headquarters. Look for a solution that delivers consistent security through remote access points or wireless WAN connectivity, without requiring intricate on-site router or security appliance installations.

7. Optimized deployment and manageability

Powerful technology that's painful to deploy and operate doesn't deliver business outcomes. The right SASE prioritizes time-to-value alongside security efficacy, and that's where a fully managed service model delivers the biggest difference.

8. Secure BYOD access

Personal devices are now part of the workforce. Modern SASE should support agentless ZTNA for identity-aware access from any device, plus a secure browser extension that embeds enforcement directly into the user's native browser experience, without forcing a costly enterprise browser rollout.

Key Board-Level Takeaways

- Legacy architectures introduce growing cyber, performance, and operational risk.
- SASE is no longer a tactical IT decision. It is a strategic business imperative.
- Network-based, fully managed SASE delivers superior security, performance, and resilience.
- Strategic partnerships enable faster, safer enterprise modernization.

What to Look for Beyond the Use Cases

The use cases tell you what the SASE service must do. The questions below tell you whether a given solution can actually deliver them at enterprise scale.

A single-vendor SASE approach

Most enterprises will run hybrid networks for years to come. Multivendor SASE re-introduces the very visibility and automation gaps SASE was meant to close. A single-vendor architecture that converges networking and security out of the box, with policies that follow the user across cloud and on-premises, is the foundation of an effective zero-trust model.

A unified agent for multiple use cases

Onboarding a different agent for ZTNA, CASB, DEM, and endpoint protection is a long-term tax on IT. The right SASE delivers all of those capabilities through a single agent and routes traffic intelligently to cloud-delivered security.

Protection for shadow IT and GenAI usage

Employees are increasingly using unsanctioned cloud applications and insecure GenAI tools, with no consideration for keeping proprietary information safe. A SASE solution should only be considered if it identifies unsanctioned cloud usage and enforces real-time policies that allow you to govern and control safe cloud usage and GenAI adoption.

AI-powered threat intelligence

Manual scripts and limited threat feeds can’t keep up with attackers who scale and adapt automatically. Effective SASE must be backed by real-time AI-powered threat intelligence to defend against all manner of threats, including the latest AI-driven attacks. Generative and agentic AI are also required to drive proactive remediation through DEM.

Top Three Questions to ask a SASE Provider

1. Is the SASE security stack truly converged with the underlying network, or is it a third-party overlay adding hops?
2. Can I get a fully managed service with 24×7 SOC support?
3. Is this a new offering, or do you have a proven SASE track record?

Why the Fortinet and Comcast Business Joint Solution Is the Answer

Most SASE offerings are pure cloud overlays. They assume your traffic should be backhauled to a third-party point of presence, secured, and forwarded on. The Fortinet and Comcast Business managed SASE solution takes a better approach.

In addition to meeting all the requirements laid out above, our network-based SASE embeds security enforcement directly into the service provider's backbone, placing protection closer to users and applications. Fortinet-powered SASE integrated directly into the Comcast Business nationwide IP network minimizes latency, reduces complexity, and ensures consistent policy enforcement. Combined with fully managed services and 24×7 security operations, you gain enterprise-grade protection without operational burden.

SASE built into the core of the Comcast network

Comcast Business operates the largest IP converged network in the United States and is the country's largest SD-WAN managed service provider. The Fortinet-powered SASE security stack is delivered directly from Comcast SASE gateways embedded in that network, so users and applications are closer together, with no extra hop through a third-party data center. The result is lower latency, consistent policy enforcement, and no hairpinning.

Security that keeps up with the speed and scale of modern attackers

Fortinet's purpose-built ASIC architecture and FortiGuard Labs threat intelligence, informed by trillions of data points, keep you ahead of known, unknown, and zero-day threats. Comcast offers a fully managed service backed by a 24×7 SOC, so you can leave security to the experts and focus on business.

Flexibility to enforce zero trust where the application lives

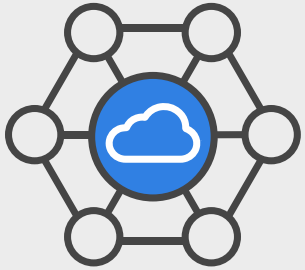
Rather than forcing every flow through a single cloud, the joint solution allows security and zero-trust enforcement to be applied close to wherever the application actually sits, delivering the best possible user experience.

A single-pane-of-glass view across your entire security fabric

With FortiManager and FortiAnalyzer, you get an end-to-end security and networking view spanning SD-WAN, switching, wireless, and SASE. This level of unified visibility cannot be replicated in a multivendor solution.

Proven scale

Over 40,000 remote sites are running on the Fortinet and Comcast Business SASE solution. The largest customer on the platform operates more than 8,000 remote locations. Comcast and Fortinet have been delivering this architecture together for more than a decade, before SASE was an industry term.



"We've built the Fortinet-powered SASE solution directly into the core of our network. That means lower latency, consistent policy enforcement, and security services that are closer to users and applications."

–Joe Austin, Vice President of Solution Engineers, Comcast Business

Choosing the Right SASE Solution

Enterprise leaders face a defining moment. Infrastructure decisions made today will shape organizational resilience, agility, and security posture for the next decade. SASE provides the architectural foundation to enable hybrid work, cloud acceleration, and secure digital growth.

However, there is great variance in SASE solutions, and it's critical to deploy a solution that can support all use cases without adding complexity. Fortinet's unique approach uses one operating system, client, and data lake, enabling true integration of zero trust, SD-WAN, and SSE. Unified management, end-to-end DEM, and consistent security policy enforcement are just a few of the benefits. The Fortinet-Comcast Business fully managed SASE offering delivers the ideal SASE solution while taking the burden off of already stretched security teams.

Learn more about Fortinet SASE.

FORTINET

www.fortinet.com

July 1, 2026 11:50 AM / MKTG-3465-0-0-EN