Three Ways Managed SASE Powers the Modern Enterprise

The Network You Have Versus the Network You Need

Your network has quietly become a business risk

There is a shift that has been happening inside most enterprises over the past five years, and it doesn't get talked about until something breaks.

For decades, "the network" was infrastructure that IT owned, leadership ignored, and the business assumed would just keep working. It was a cost line, not a conversation. Then the work moved to the cloud, the workforce moved everywhere, the threat landscape changed shape, and AI walked through the door. The network is now the layer that has to make all of that work. Every day, securely, at scale, for users who notice every millisecond of delay.

That shift has consequences most leaders haven't fully budgeted for. 35% of CSOs say the cost of network outages to their organization runs between $1 million and $5 million annually.[1] Meanwhile, enterprise network traffic is projected to grow 27% annually through 2026, driven by AI workloads, video conferencing, and IoT expansion.[2]

The network you built for the workload you had is being asked to carry a workload it was never designed for, on a curve that doesn't flatten.

A network that was once a quiet cost line has become a strategic variable. Now the question is whether your current architecture is keeping up, or whether it is quietly stifling what your business can do next.

In this eBook, we'll examine why the way most organizations operate their networking and security stacks has become the problem itself, and how that operating-model problem now ripples into resilience, performance, AI readiness, and team capacity. We'll introduce Secure Access Service Edge (SASE) as the architectural response, walk through three specific outcomes it delivers for the business, and provide practical guidance on what to look for in a Managed SASE partner and how to phase the move into the strategy you're already running.

It's likely that most of you reading this (if not all of you) are probably not running a greenfield architecture. Your network is more likely a patchwork of MPLS lines that were supposed to be retired three years ago, software-defined wide area network (SD-WAN) trials that became partial deployments, multiple generations of VPNs, legacy firewalls a previous IT director picked, and a couple of cloud-native experiments running alongside it all.

That patchwork you are responsible to manage, and ensure evolves with the business, is in essence the protagonist. We've written this eBook assuming you're starting from where you actually are, not from where some vendor diagram suggests you should be. And so, we begin with where most of the pressures on your existing network are actually coming from.

[1]Opengear, A Global Report on Network Management: Building AI-Ready Resilience in Data Centers (2025)
[2]IDC, Global DataSphere Report (2025)

The Fragmentation Tax

Walk into any enterprise IT environment and you will find the same picture. Multiple consoles for tools that were supposed to talk to each other. Policies that mean slightly different things in slightly different places. Change windows that take weeks because three teams have to coordinate. Alerts arriving from four directions that may or may not be describing the same incident. And a quiet, growing list of point solutions no one fully owns.

Take the example of what modern cybersecurity looks like after a decade of buying one tool at a time. 51% of enterprises now run 11 or more distinct security tools.[3] Each one was bought for a reason. Most of them work. Almost none of them work together. This same gap exists between tools well beyond just cybersecurity, extending the lack of true visibility and manageability into the network and every aspect of operations the network touches.

The visibility cost itself shows up in the data. 27% of IT respondents cite network visibility as a top operational challenge.[4] 38.4% of network operations organizations cite lack of end-to-end visibility across network domains as one of the biggest challenges to success.[5] Another way of putting it is that more than a third of network teams are operating with documented blind spots they can't close with the tools they have.

The hard truth: more tools haven't necessarily produced more security, productivity, or efficacy. But they definitely have produced more complexity, more places to fail, and a greater chance of operational issues as business needs change.

[3]Purple Book Community, The State of AI Risk Management (2026)

[4]Auvik, Beyond the Hype: The Real State of IT (2026)

[5]EMA (Enterprise Management Associates), Network Management Megatrends 2026: Automation, Hybrid and Multi-Cloud Networks, and AI Transformation (2026)

The Cyber Resilience Gap

Most security strategies are still organized around the idea that prevention is the goal. Stop the bad thing before it happens, and you've already won. That model worked when attackers moved slowly and stayed put once they got in. It doesn't fit the reality your team is operating in now.

Consider what the numbers say about how this actually plays out. The mean time to detection (MTTD) of an incident is 277 days.[6] Most attackers move laterally across your network throughout that window. The average cost of a data breach has reached $4.44 million.[7] Credential abuse accounts for 32% of breaches,[8] meaning roughly a third of incidents start with attackers walking in through legitimate access paths your network is built to trust. And once they are in, recovery is no guarantee: among ransomware-affected organizations, only 28% fully recover all affected data.[9]

277 Days
Mean time to detection of an incident

$4.44M
Average cost of a data breach

32%
Breaches from credential abuse

72%
Ransomware-affected organizations that don't fully recover

Read those numbers in sequence. Attackers are already inside, and they're using credentials your network trusts. Most organizations don't fully recover when something goes wrong. A security posture built only on prevention is, by definition, planning to win the first round and then losing the rest.

The hardest conversation in incident response isn't with the attacker. It's the one the security lead has with leadership the next morning, trying to explain why detection took as long as it did. The honest answer is usually that the data was spread across five tools that don't agree with each other, and stitching it together while the incident was in motion was an exercise in archaeology.

Cyber resilience is the recognition that prevention, detection, containment, and recovery are now one continuous problem. The network is the layer that runs through every part of it. A strategy that treats those as separate projects, owned by separate tools, is a strategy with built-in seams. The data above is what those seams look like in production.

[6]Fortinet, State of Cloud Security Report (2026)
[7]Immersive, From Compliant to Capable in an AI-Driven World (2026)
[8]Verizon, 2025 Data Breach Investigations Report (DBIR) (2025)
[9]Veeam, 2026 Data Trust & Resilience Report (2026)

The AI Readiness Problem

Every executive conversation right now ends up at AI. And nearly every AI initiative, once it gets past the slide/strategy phase, runs into the same wall: the network underneath it wasn't designed for what AI does.

The teams responsible for running the network already see it coming. 38% of network professionals cite congested traffic flows as a networking challenge that will impact their organization's success with AI.[10] 34% point to unpredictable traffic bursts.[10] Those aren't theoretical concerns. They're network engineers telling you that the foundation underneath the AI strategy is not ready to carry it.

The AI strategy gets approved at the board level on a quarterly timeline. The network gets asked to support it on next month's timeline. Those two timelines were not coordinated with each other, and the network team is the one holding the gap.

The infrastructure gap shows up at the executive level too. 44% of executives are now conducting enterprise-wide infrastructure assessments specifically to identify gaps that could limit future AI capabilities.[11] There is a reason for the urgency: organizations with more mature AI governance see an 18% increase in AI adoption.[12] Governance starts with knowing what your traffic is doing, which most networks today simply cannot tell you.

And then there is the part of AI use that nobody put on the roadmap. 49% of employees are already using AI tools their employer hasn't approved.[12] Sensitive data is leaving the organization on paths IT did not design and does not monitor, while the official AI program is still in pilot.

AI is not the thing that will eventually stress your network. It is the thing already exposing what your network can't do.

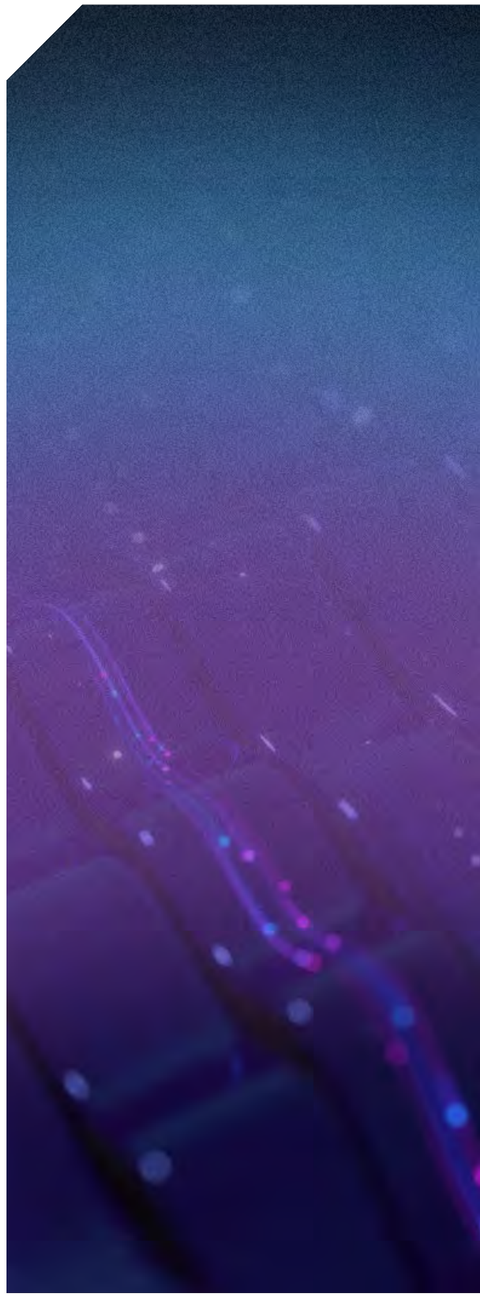
The Skills and Operations Squeeze

If the technology problem is hard, the staffing problem is harder. 74% of organizations report an active shortage of cybersecurity talent.[13] Over half of enterprises struggle to hire and retain skilled network engineers,[5] particularly in the areas that matter most right now: security, AI networking, and automation. The people who could untangle the stack you have today are the same people every other organization is also trying to hire.

Hiring a senior network engineer with security depth takes six months on a good day, and most teams don't get a good day. The engineers who could untangle the stack you have are interviewing at three other companies this week.

And the team you do have is paying the cost. 79% of security professionals say job stress takes a toll on their physical and mental health.[14] Burnout is not a personality issue; it is the predictable outcome of asking a smaller team to operate a more complex environment under faster-moving threats with fewer hours in the day.

You can buy more tools. You cannot buy more time. Even if you could solve the technology problem with budget, you cannot solve the operations problem with budget. Not at the rate the problem is moving. Not on the timeline the business expects.



[10]Broadcom (Network Observability), The State of Network Operations (2025)
[11]Hakkoda, 2026 State of Data Report (2026)
[12]BlackFog, The State of Ransomware Q1 (2026)
[13]Fortinet, 2026 Cloud Security Report: Closing the Cloud Complexity Gap (2026)
[14]Ivanti, 2026 State of Cybersecurity Report: Bridging the Divide (2025)

So, What Now?

Here's where this leaves your organization. The stack is fragmented. Prevention isn't enough. AI is exposing every weakness in the network at once. And the team you'd ask to fix it is already over capacity.

The instinct in most organizations is to keep solving this one tool at a time. Another point product here. Another patch there. That instinct is what got everyone where they are now.

The question worth asking is different: what would it look like to solve this as one problem instead of 15?

The answer the industry has been converging on for the past five years isn't another product. It's a different operating model: a single, cloud-delivered architecture that pulls networking and security together rather than running them as parallel stacks, delivered as a managed service so the operational burden doesn't land back on your team.

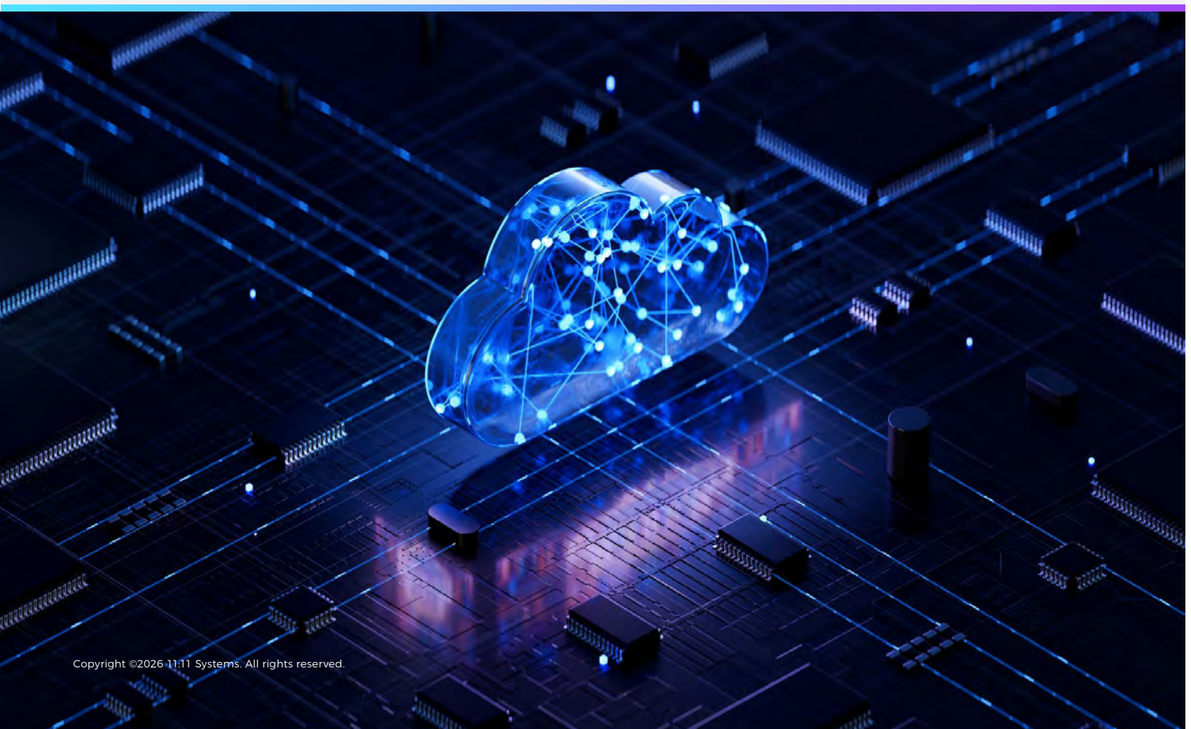
The shorthand for that operating model is Managed SASE. The remainder of this eBook focuses on three outcomes you can expect from it, and how to begin a plan to incorporate Managed SASE into your existing strategy.

What we mean by Managed SASE

SASE, or Secure Access Service Edge, is the architectural convergence of networking and security into a single, cloud-delivered service. Instead of running tools like Software-Defined Wide Area Network (SD-WAN), Zero Trust Network Access (ZTNA), firewalls, secure web gateways, Cloud Access Security Broker (CASB), and threat protection as separate stacks, SASE puts them on one platform, with one policy plane, applied consistently to every user, every site, and every cloud destination.

Managed SASE means a provider operates that platform end-to-end on your behalf: the underlay, the SD-WAN, the SASE overlay, the monitoring, and the response. You consume the outcome, not the project.

That distinction matters for the rest of this eBook, because the three outcomes Managed SASE delivers all depend on it.



Three Outcomes Managed SASE Delivers

Usually, a single solution can't solve all of an organization's problems. The problems themselves are too varied, the systems too interconnected, and the constraints too different for any one tool to address all of them at once.

SASE is the exception, and not because it's a single solution. It's the exception because it isn't one. SASE is a category that brings together a wide range of networking and security functions that used to live in entirely separate stacks: secure connectivity, identity-aware access, application-aware traffic optimization, threat prevention, data protection, cloud on-ramps, and the operational fabric that holds it all together. It sits at the intersection of networking, security, and the cloud, which means it can address business concerns that span all three at once.

That breadth is why Managed SASE shows up in conversations about resilience, performance, and operational capacity, often at the same time. To better explain how Managed SASE can impact many parts of your operation, let's look at three outcomes organizations using Managed SASE experience.

OUTCOME 1

Strengthened Cyber Resilience

OUTCOME 2

Optimized Network Performance for What's Next

OUTCOME 3

Managed. Not Manual

OUTCOME 1

Strengthened Cyber Resilience

The first business outcome SASE delivers is the one most directly tied to the cyber resilience gap previously mentioned. It isn't a single SASE capability that helps achieve the outcome; it's a set of architectural shifts that compound, each one closing a specific cybersecurity failure that fragmented stacks have only made worse.

Convergence Shrinks the Attack Surface.

A unified SASE policy plane eliminates the spaces between tools where attackers and audit findings both tend to live. The fragmentation tax stops compounding because there is no fragmentation to tax. One policy, applied consistently across every site, every user, and every cloud destination. Not 11 policies trying to agree on what "permit" means. The practical effect is that the number of places a misconfiguration can hide drops by an order of magnitude, and the policy you wrote down is the policy actually enforced everywhere.

Zero Trust Replaces Implicit Trust.

ZTNA changes the access model from "you're inside the network, so you're trusted" to "you're authenticated for this specific application, in this specific context, right now, and we will re-evaluate that on the next request." That single shift addresses two problems at once. The credential abuse problem noted earlier (where 32% of breaches start with legitimate-looking access) gets contained, because compromised credentials no longer grant the freedom to move laterally. And the remote workforce problem gets simpler, because the network perimeter you can't draw is no longer the thing access depends on. Identity is the perimeter, and the policy enforces it everywhere.

Segmentation Contains the Blast Radius.

Beyond keeping attackers out, SASE shrinks what they can reach once they're in. Microsegmentation and ZTNA work together to scope every session to a specific application in a specific context, which means a compromised credential, a compromised endpoint, or a compromised workload doesn't get to wander. Resilience isn't just preventing the worst case. It's making sure the worst case stays a small case.

Faster Detection, Faster Response.

A unified SASE solution produces one telemetry stream from one data lake, instead of five disconnected Security Information and Event Management (SIEM) feeds your team has to stitch together at 2 a.m. while an incident is in motion. Layer AI-driven analytics on top, with pattern detection, anomaly scoring, and threat hunting running across all of it, and both time-to-detect and time-to-contain compress in one motion. Detection becomes a property of the platform rather than a project the team has to run.

The Network Stays Stable throughout the Incident.

When a fragmented stack is responding to an incident, the network itself often becomes part of the problem. Policy changes get pushed inconsistently, segments fall offline as teams try to isolate the blast, and the troubleshooting paths the response depends on are themselves degraded. A unified SASE solution keeps the access fabric stable while response is in motion. Policy can be tightened in one place and propagated uniformly. The parts of the environment that aren't part of the incident keep working. The response team isn't fighting the network at the same time as the incident.

Resilience after the Incident.

Here's the part most resilience strategies miss. Every recovery plan assumes the network you'll recover over is still trustworthy. Most aren't, because the same fragmented stack that let the incident happen is the one disaster recovery (DR) depends on. A unified solution keeps the path to clean backups, immutable storage, DR sites, and recovery environments inside the same security boundary. The infrastructure you depend on to recover isn't the same infrastructure the attacker just compromised. When the prevention layer fails, the resilience layer needs to be intact. With SASE, they're the same layer.

Forensic Continuity Makes the Response Defensible.

Resilience isn't just recovering from an incident. It's being able to reconstruct what happened, when, and what was touched. A single SASE telemetry stream produces a coherent audit trail across user, network, and application. Fragmented stacks produce fragmented trails that compliance teams and forensic investigators have to stitch together after the fact, often under time pressure and with incomplete data. With SASE, the timeline is already assembled.

This is why SASE shows up in cyber resilience conversations, not just security conversations. Resilience isn't a posture you can buy as a separate product. It's the network behaving consistently before, during, and after an incident. SASE is what makes "the network behaving consistently" something you can architect, rather than hope, for.

OUTCOME 2

Optimized Network Performance for What's Next

The second business outcome is performance. This is where SASE's architectural shift matters most, because it changes what performance even means.

SASE Changes the Performance Equation.

Traditional network architectures forced a choice. You could route traffic through a central inspection point and have security but pay the latency cost. Or you could let traffic break out locally and have speed but lose visibility. SASE eliminates that choice by moving inspection and policy enforcement out of centralized data center appliances and into a distributed edge close to users, sites, and workloads. Security travels with the traffic. The secure path is the fast path. Everything else in this pillar builds on that.

SD-WAN Turns the SASE Fabric into Intelligent Connectivity.

Once you have a converged secure fabric, SD-WAN becomes the layer that decides how each session traverses it, application by application, in real time. Application-aware routing, dynamic path selection across whatever transports are available, self-healing failover. SD-WAN on top of SASE can make pure performance decisions because security doesn't have to be reconsidered with each routing choice. It's already enforced.

Intelligent Traffic Steering Puts the Right Traffic on the Right Path.

Building on SD-WAN, steering uses what the SASE platform already knows about application identity, user context, and risk to make finer-grained decisions: which sessions get the private backbone, which can take direct internet breakout, which require deeper inspection. None of those decisions are possible without unified policy and telemetry. The SASE foundation provides exactly that.

The Global Private Backbone Delivers Predictable Performance at Scale.

A SASE-aligned backbone gives SD-WAN and steering a high-quality, SLA-backed path to use when it matters. Because the backbone is part of the same unified solution , traffic doesn't exit one security boundary to enter another to reach it. That eliminates the latency and policy stitching that have historically made private backbones expensive to operate at scale.

Direct Cloud On-Ramps Optimize for Where Work Actually Happens.

SASE's distributed edge enables direct, secured on-ramps into the major cloud providers and Software as a Service (SaaS) platforms. SaaS and multi-cloud traffic take the shortest performant path instead of being backhauled through a data center. Users get the experience they expect. IT keeps the visibility and control that backhauling used to provide. The trade-off goes away.

AI Initiatives Become Viable and Governable.

This is the pillar's most timely point. It's also the one that closes the loop on the AI readiness problem already discussed. AI workloads stress every layer of the network at once: bandwidth to data sources, latency to inference endpoints, visibility into sanctioned and unsanctioned GenAI usage, and governance over what data leaves the organization.

Because the SASE foundation already converges performance and security at the edge, and because SD-WAN, traffic steering, the backbone, and cloud on-ramps all build on it, the same architecture optimizing today's traffic is the one positioned to make AI initiatives operationally viable and governable. The infrastructure assessment we mentioned that 44% of executives are running right now? *This* is what they're looking for.

OUTCOME 3

Managed. Not Manual

The third outcome is the one most often left out of SASE conversations. It also determines whether the other two actually materialize.

Day-One Access to Deep Expertise.

SASE done well requires deep networking and deep security skills, available 24x7x365, to support an environment that doesn't sleep. The massive talent shortage organizations are experiencing isn't a hiring inconvenience. It's a structural reality. Most organizations cannot realistically build that bench, retain it, and keep it current. A managed model closes the gap on day one, not in two years and three rounds of recruiting.

Continuous Operations, without Continuous Overhead.

A follow-the-sun Network Operations Center (NOC) and Security Operations Center (SOC) isn't a feature. It's the day-to-day operational fabric of running a SASE platform well. Proactive monitoring, threat hunting, change management, capacity planning, incident response, carrier escalation. This is the work that doesn't show up in product comparison sheets but determines whether the platform delivers on the promises in the brochure. With a managed provider, that work is happening whether your team is in the office or asleep.

One Provider Owns the Outcome.

There is a meaningful operational difference between owning a SASE outcome and owning a vendor relationship. When one provider is responsible for underlay, SD-WAN, and the SASE overlay, there is no finger-pointing between carrier, network vendor, and security vendor when something breaks. One contract. One SLA framework. One escalation path. One bill. That's not a tagline; it's the operational reality that determines whether incidents get resolved in two hours or two days.

Internal Capacity, Reclaimed for Strategic Work.

This often undersold benefit of managed delivery is the one finance teams should care about most. When day-to-day SASE operations move to a managed provider, the internal team gets back the hours they were spending on routine maintenance, ticket triage, and change windows. Those hours flow back to the projects the business actually values: AI rollouts, cloud migrations, application modernization, the things on the strategic plan that everyone agrees matter but nobody has time to execute. The team you couldn't afford to staff up gets effectively bigger.

Three Outcomes, One Compounded Effect

These three outcomes aren't independent. They're a system.

Better performance is what makes AI initiatives operationally viable. Wider AI adoption is what makes resilience non-optional. Resilience and performance both depend on disciplined daily operations, which is what the managed model delivers. The architectural shift that strengthens resilience is the same shift that improves performance, and the operations model that supports both is the one that frees your team to do something other than fight tools.

That's why the conversation has moved from "should we adopt SASE" to "how should we operate it."

OUTCOME 1

Strengthened Cyber Resilience

OUTCOME 2

Optimized Network Performance for What's Next

OUTCOME 3

Mangaged. Not Manual

Making the Move

Readers of this eBook will be in very different places. Some are just starting to map their network and security gaps against where the business needs to go. Others are mid-evaluation, weighing platforms, partners, and timing. A few are already running a SASE rollout and trying to figure out what success should look like.

Wherever you are, the move toward Managed SASE isn't usually a singular decision. It's a series of smaller decisions that compound, made over a period of months as the picture sharpens. So, let's take a look at three questions you should be asking yourself (on behalf of your organization) to help you better crystalize your next step.

How Does Managed SASE Fit the Strategy You're Already Running?

Most buyers have an unspoken concern at this point in the conversation, and it's worth naming directly: does this replace what I've already built, or does it extend it?

The honest answer is the latter, when it's done right.

Managed SASE doesn't replace your identity provider, your endpoint security stack, your cloud security tooling, or your disaster recovery program. It complements them. Identity tells SASE who someone is; SASE enforces what they can access. Endpoint tools protect the device; SASE protects the connection between the device and the application. Cloud security protects what runs in the cloud; SASE secures the path to it. Disaster recovery restores the workloads; SASE makes sure the recovery network is still trustworthy when you need it. Each of these investments gets more value when the network underneath is converged and consistent, not less.

The deployment path should reflect that. You don't have to rip and replace. A well-structured Managed SASE rollout is phased: remote workforce first, where the value is fastest and the disruption is lowest. Then branch sites, retiring legacy VPN and point-firewall investments as you go. Then full convergence, with overlapping security and networking tools retired on a schedule that matches the depreciation curve.

Change management is real. Any architectural shift touches process, ownership, and skill sets. But it's bounded. The phased model means the business sees value within a quarter, not within a multi-year project. That's how organizations are moving to Managed SASE now: not as an enterprise transformation initiative, but as a series of bounded steps, each of which earns the next one.

What Does “Good” Look Like in a Managed SASE Partner?

Once you’ve decided Managed SASE fits, the next question is who delivers it. Here’s a buyer’s lens that holds regardless of which underlying SASE platform a provider runs. Each of these is a commitment, not a feature.

- **A truly unified platform, not bundled point products.** Ask whether the SASE platform was built as one platform or assembled from acquisitions. The difference shows up in policy consistency, telemetry, and time-to-investigate during incidents. Convergence is the whole point. Bundles don’t deliver it.
- **End-to-end ownership of underlay, SD-WAN, and SASE overlay.** A provider that manages only the overlay while the customer manages the carriers and circuits has not solved the accountability problem. Single-provider accountability requires single-provider responsibility, all the way down to the last mile.
- **A 24x7x365 NOC and SOC with named SLAs.** Operations is where most SASE deployments quietly fail. Ask what the NOC and SOC actually do, who staffs them, where they sit, and what the SLAs commit to. Vague answers here predict vague outcomes later.
- **Carrier and connectivity flexibility.** A carrier-agnostic underlay with broad reach across hundreds of carriers, spanning fiber, broadband, 5G, and satellite, is what keeps you from being constrained by your provider’s preferred relationships in markets where they don’t have leverage.
- **Integration with your existing IT Service Management (ITSM) workflows.** Alerts, incidents, and change control need to flow into the tools your team already uses: ServiceNow, Jira, whatever you’ve standardized on. Without that, “managed” becomes a parallel operational track instead of an integrated one.
- **Transparent visibility and reporting through a single portal.** You should not have to call your provider to know how your network is performing. A single pane of glass across performance, SLAs, security events, and incidents is table stakes.
- **A roadmap that includes AI security and governance.** The next 24 months of SASE will be defined by how well platforms handle AI traffic: visibility into GenAI use, control over data flowing to external models, governance over agentic workflows. Ask what’s on the roadmap.

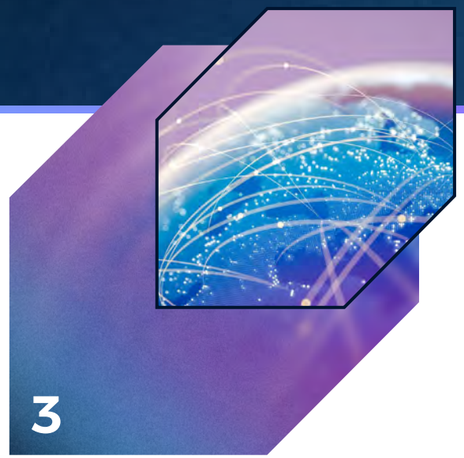
Why 11:11 Systems?

This is where 11:11 fits into the conversation. Managed SASE is one component of 11:11's Resilient Cloud Platform, the broader portfolio of services that connect, protect, and recover the modern enterprise. That context matters. Cyber resilience isn't a single product; it's a posture maintained across networking, cloud, security, and recovery, and 11:11 builds toward that whole.

A few specifics worth knowing:

The underlying SASE platform is delivered in partnership with Cato Networks, a recognized leader in unified SASE. The delivery model is designed to remain flexible as 11:11's portfolio expands, so the architectural decisions you make today don't lock you into a single vendor's roadmap.

11:11's in-house NOC operates 24x7x365, with SLA-backed monitoring, incident response, and change management across the entire stack: underlay, SD-WAN, and SASE overlay.



The underlay is carrier-agnostic, with access to more than 200 global carriers and the full range of access technologies, including fiber, broadband, 5G, and satellite. Connectivity decisions are made on what's best for each site, not what's most convenient for the provider.

The broader portfolio. Managed SASE sits alongside 11:11's connectivity, cloud, and recovery services, so the cyber resilience story isn't a story you have to assemble from multiple providers.

The Business Case in Five Points

If you read nothing else, these are the five things worth taking to your next leadership conversation.

1 Fragmentation Is Now the Risk, Not the Safeguard.

Using a large number of disparate tools haven't made anyone safer or more productive; they've made it harder to manage. Convergence is the response.

2 Resilience Is a Network Problem as Much as a Security Problem.

Prevention, detection, containment, and recovery all run through the network. They need to behave like one system, because they are one.

3 AI Initiatives Will Expose Whichever Piece of Your Infrastructure Is Weakest.

The network is usually that piece.
Address it before the AI roadmap does it for you.

4 Convergence and Managed Delivery Are How Leading Organizations Are Responding.

Not as a transformation project, but as a phased architectural decision, one that pays off within a quarter, not a fiscal year.

5 The Right Partner Makes This an Operational Upgrade, Not a Multi-Year Project.

Single-provider accountability, an in-house NOC and SOC, and a carrier-agnostic underlay are the difference between a SASE deployment that works and one that drags.

The Next Step

The hardest part of moving to Managed SASE is usually the conversation that gets it started. We'd suggest making that the easy part.

Talk to 11:11 Systems about where your network is today, what your AI and cyber resilience priorities are over the next 12 months, and what a phased path to Managed SASE could look like for your environment. One conversation. No multi-year commitment to start.