



MOMENTUM
EMEA

EBOOK ONE OF THREE

MODERNIZING ENTERPRISE IT

How to build a strong foundation with SASE

Why legacy networks can't keep up, and how Secure Access Service Edge gives IT leaders a unified, cloud-delivered foundation for connectivity and security.

Table of contents

03 The stakes have changed

04 Why transform now?

05 Proof the risk is real

06 Building resilient, agile
infrastructure

07 SASE fundamentals

08 What SASE replaces

09 Core principles of SASE

10 Real business outcomes of SASE

11 Setting the foundation for a
smarter network

12 Ready to get started?

THE STAKES HAVE CHANGED

Here's why your network can't stay the same

Enterprise IT has evolved beyond simple uptime. Today, it's about delivering seamless experiences, robust security, and rapid adaptability, simultaneously, across diverse environments.

Employees demand flawless access, whether they're working remotely, traveling, or on-site. Applications are dispersed across multiple clouds and data centers. Cyberattacks have become more sophisticated, leveraging automation and AI to exploit vulnerabilities swiftly. Meanwhile, budgets remain constrained, and compliance requirements intensify. The traditional patchwork of routers, firewalls, and manual processes is no longer cutting it.

Modern enterprises need infrastructure that's intelligent, adaptive, and resilient. This eBook, the first in a three-part series on modernizing enterprise IT, explores how IT leaders can navigate these challenges by embracing:

SASE: integrating connectivity and security into a unified, cloud-delivered framework.

AI-driven operations: predicting and mitigating issues proactively.

Security automation: responding to threats in real time, reducing manual intervention.

IBM COST OF A DATA BREACH 2024

\$4.88M

Global average data breach cost in 2024, up 10% year over year, the highest on record.

\$2.22M

Average cost reduction for organizations using security AI and automation extensively.

\$6.08M

Average breach cost in financial services, 22% above the global average.

WHY TRANSFORM NOW?

The evolving enterprise network

Enterprise IT is no longer judged by uptime alone. It's measured by user experience, threat resilience, and the ability to adapt in real time. Traditional architectures like static MPLS networks, standalone firewalls, and siloed visibility were never built for this, and the gap between what users expect and what these legacy systems can deliver grows wider every year.

When remote work expanded overnight, most enterprises bolted on VPNs. When cloud applications exploded, most layered new security tools over old frameworks. The results: fragmented policies, blind spots between environments, and manual processes that simply can't scale.

Meanwhile, attackers have already evolved. Ransomware groups operate with AI, automation, and global playbooks. They move faster than your change approvals, and count on that delay. When your network can't adapt instantly, threats don't knock louder, they walk right in. This isn't about modernization for its own sake. Today, the focus is on survival.

277 days is the average time to detect and contain a breach, nearly nine months of silent exposure.

74% of breaches now involve the human element, phishing, stolen credentials, or mistakes amplified by remote work.



Legacy networks are a ticking clock.

Downtime costs enterprises an average of \$12,900 per minute, and attackers now move faster than most change-approval processes.

PROOF THE RISK IS REAL

The executive mandate: why IT transformation is now a board-level priority

For years, IT was seen as a back-office function, a cost center, not a value driver. Today, that's changed. Boards and CEOs are now asking blunt questions: "How fast can we expand securely to new markets?" "What happens if ransomware hits us tomorrow?" "Are we breach-ready, or breach-deniable?"

Regulators such as GDPR, CCPA and HIPAA no longer see breaches as bad luck, they treat them as a failure to meet basic operational duty. Customers are abandoning companies faster than ever after breaches, and cyber insurance carriers are raising premiums or denying coverage entirely for companies that cannot prove proactive, automated defenses. In short, doing nothing is no longer a neutral stance, it's reckless.

You don't need a breach to expose your risk. Delays in updating architecture already put you behind in security, compliance, and business agility.

41%

of consumers say they would immediately stop doing business with a breached company.

63%

spike in credential-based breaches among enterprises relying heavily on traditional VPN architectures.

80%

of IT leaders say their current network security model isn't sustainable for hybrid work and cloud-first environments.

WHAT'S NEXT

Building resilient, agile infrastructure

If the traditional model is collapsing, what replaces it? The answer isn't more isolated tools. It's an architecture built to:

- 1 Unify security and connectivity across cloud, edge, and user devices.
- 2 Enforce identity-based policies everywhere.
- 3 Move and adapt as fast as the business needs.

That's why the next chapter focuses on SASE, the strategic convergence of networking and security for a borderless enterprise.

SASE FUNDAMENTALS

SASE fundamentals for secure, streamlined connectivity

The modern enterprise no longer operates within clear walls, data centers, or user boundaries. Employees connect from everywhere. Applications live across SaaS, private cloud, and public cloud. Cyber threats move faster than any human team can respond.

Trying to bolt security and connectivity onto this new world with traditional VPNs, MPLS lines, and hardware firewalls only guarantees complexity, gaps, and failure. SASE changes that. Instead of layering more hardware and manual policies, SASE converges security and connectivity into one seamless, cloud-native fabric that:

- Follows users wherever they work.

- Protects applications wherever they live.

- Simplifies IT operations rather than making them harder.

70%

of enterprises will have explicit SASE adoption strategies by 2025, up from less than 10% in 2020 (Gartner).

This isn't an emerging trend anymore. It's the new minimum standard, and it's already happening.

WHAT SASE REPLACES

What SASE replaces, and why it matters

Without SASE, most enterprises are stuck with fragmented security policies (one set for VPN, another for on-prem apps, another for SaaS tools), backhauling inefficiency that adds latency and risk, visibility gaps that leave IT unable to see how users access critical apps, and inconsistent identity controls that trust users based on IP address instead of continuous verification.

Every one of these gaps is a door left unlocked for attackers. For example, imagine a multinational company backhauling all remote user traffic through its HQ firewall. This decision led to a \$3.4 million ransomware breach because employees bypassed the VPN due to slowdowns, exposing cloud apps without monitoring.

SASE prevents this by delivering:

Cloud-native security controls at Points of Presence (PoPs) around the world.

Direct-to-cloud traffic routing without risking exposure.

Consistent, identity-driven policies no matter where the user or app is located.



\$3.4 million in ransomware losses, traced back to one backhauling decision.

Every fragmented policy and visibility gap is a door left unlocked for attackers.

CORE PRINCIPLES OF SASE

Core principles of SASE

PRINCIPLE	WHY IT MATTERS
Identity-driven access	Users, devices, and apps are authenticated and verified continuously, not just at login.
Cloud-native architecture	Security services are delivered from the cloud, reducing hardware dependency and latency.
Unified policy management	A single policy framework governs all users and apps, no matter their location or device.
Distributed enforcement	Traffic inspection happens closest to the user or app, not funneled through a bottleneck.
Resilient global coverage	Secure access must work at high performance across continents, not just cities.

Together, these five principles replace the fragmented patchwork of VPNs, MPLS lines, and standalone firewalls with one adaptive, identity-aware fabric.

REAL BUSINESS OUTCOMES OF SASE

The real business outcomes of SASE

107% ROI over three years, with a net present value of \$9.49 million.	46% fewer security incidents year over year for full SASE adopters.	30% average improvement in application performance after removing VPN backhauling (Gartner 2024).
--	---	---

SASE gives enterprises the architecture they need to secure, connect, and scale more effectively. But the foundation is just the first step. To fully modernize operations, organizations also need to rethink how they manage, troubleshoot, and respond, shifting from reactive processes to intelligent, automated workflows.

SASE READINESS SELF-CHECK

- Your users complain about app slowness or VPN pain.
- Your IT team struggles to see and enforce security in SaaS platforms.
- Your budget can't keep up with endless hardware refreshes.
- You lack unified identity controls across your environments.

WHAT'S NEXT

From simpler architecture to smarter operations: eBook two explores how AI and automation help IT move faster and respond smarter.

SETTING THE FOUNDATION FOR A SMARTER NETWORK

Setting the foundation for a smarter network

Legacy infrastructure is holding businesses back. It's costly, brittle, and too slow to respond to modern demands. In these first chapters, we laid out why transformation is no longer optional and why SASE is the strategic foundation for building a network that's flexible, secure, and built for scale.

SASE simplifies the architecture. It closes visibility gaps, strengthens security, and prepares the enterprise for what comes next. But architecture alone isn't enough. Once the foundation is in place, the next challenge is operating smarter, reducing manual tasks, responding faster, and giving IT teams the visibility and control they need to move at the pace of the business.

That's exactly what we cover in *AI and automation for enterprise IT*, eBook two in this series, which explores how to go from reactive to resilient, and what that looks like in practice for IT.

KEY TAKEAWAY

A converged, identity-driven SASE architecture is the foundation. Smarter, automated operations are what you build on top of it.

READY TO GET STARTED?

Book a call and discover how a single, converged SASE architecture unifies your networking and security.

Momentum, in partnership with Cato Networks, helps organizations replace fragmented VPNs and firewalls with one cloud-delivered platform for connectivity and security.

[Book a call](#)

MOMENTUM EMEA

Horapark 3, 6717 LZ Ede
+31 (0)20 226 1500
service@gomomentum.eu
gomomentum.eu

eBook one of three · Modernizing enterprise IT
Next: AI and automation for enterprise IT