MOMENTUM
EMEA

EBOOK TWO OF THREE

MODERNIZING ENTERPRISE IT

AI and automation for enterprise IT

Smarter networks, faster teams. How AI-driven networking and cybersecurity automation turn a SASE foundation into a real operational advantage.

Secure · SASE & SSE

gomomentum.eu

Table of contents

PART TWO OF THREE

AI and automation for enterprise IT

In Part 1 of this series, we made the case for replacing legacy infrastructure and outlined how Secure Access Service Edge (SASE) provides the architectural foundation for a more scalable, resilient enterprise.

A stronger foundation is only part of the equation. To fully modernize IT, organizations must rethink how their environments are operated, managed, and secured. The traditional model of fragmented visibility, reactive troubleshooting, and manual response workflows can't scale to meet today's demands.

This guide focuses on what comes next. We'll examine how AI-driven networking and security automation are transforming day-to-day operations, capabilities that reduce complexity, accelerate issue resolution, and give IT teams the intelligence and control they need to support the business at speed.

> "
>
> **As pressure grows to do more with less, operational intelligence becomes the next competitive differentiator.**

AI-DRIVEN NETWORKING

Going beyond manual operations

IT teams today do not fail because they lack effort. They fail because the systems they manage outscale human capacity: thousands of devices across hybrid clouds and campuses, millions of telemetry points every hour, and endless alerts competing for attention.

Manual processes simply cannot keep up, change windows stretch for weeks, and configuration drift creeps in unnoticed. According to IDC's 2024 Network Intelligence Report, enterprises still relying on manual network management report MTTR (mean time to resolution) averages of up to 9 hours per incident. That delay doesn't just impact IT metrics, it drags down employee productivity, customer experience, and business outcomes.

AI-driven networking was not designed to replace people. It was built to help teams move at machine speed, not human speed. Done right, it changes the entire rhythm of network operations by:

- Ingesting real-time telemetry from switches, routers, and access points, and correlating anomalies automatically.
- Quantifying user experience through Service Level Expectations (SLEs) and proactively recommending fixes.
- Enabling natural language queries instead of complex CLI commands.

90%

faster issue resolution for companies adopting AI-driven network analytics, versus peers using traditional methods (Gartner 2024 AI-ops report).

9 hours: the average MTTR under manual network management, per IDC's 2024 Network Intelligence Report.

OLD WAY VS. NEW WAY

A quick comparison

What does this look like in practice? A finance company's remote office starts experiencing Wi-Fi dropouts every afternoon.

UNDER THE MANUAL MODEL

Users flood the help desk with tickets.

IT staff manually gather logs from access points, controllers, and client devices.

It takes hours to correlate the symptoms to a misconfigured DHCP setting.

In the meantime, client frustration builds and productivity drops.

UNDER THE AI-DRIVEN MODEL

The network continuously streams telemetry to a centralized AI engine.

The system detects a spike in DHCP failures around 2 PM daily.

An automated alert is generated, with probable root cause, DHCP pool exhaustion.

A recommended fix is sent to IT staff, who validate and apply it before most users notice.

Under the manual model there's an influx of support tickets, lost hours, and drops in productivity. This shift is why IDC found enterprises deploying AI analytics cut MTTR by up to **60%** in 2024.

PROOF IT WORKS

Measurable outcomes, and what AI cannot do yet

The promise of AI in networking is no longer theoretical, it's already backed by real business outcomes. Unified visibility and centralized management, key pillars of AI-driven networking, have led to faster new site deployments, fewer emergency change windows, and clearer SLA reporting to business stakeholders.

AI-driven operations also reduce operational burnout. Instead of drowning in alerts, IT teams spend more time optimizing and innovating, and the number of low-value tickets handled by Tier 1 help desks drops sharply.

While AI transforms operations, it is not a replacement for skilled IT professionals. AI can spot anomalies, recommend fixes, and automate routine tasks, but it still requires:

- Capable engineers to validate critical changes.
- Human oversight for exceptions and new situations.
- Strategic planning beyond algorithmic recommendations.

75%

of enterprises reported improvements in customer experience and employee satisfaction within 18 months of deploying AI-driven networking (Forrester 2024).

Over-reliance on "self-driving" networks without governance creates new risks, especially in regulated industries where auditability matters. The most successful teams see AI as a force multiplier, not a crutch.

TAKING THE NEXT STEP

Cybersecurity automation

Enterprise networks today face attacks that move faster than human teams can respond, especially with the rise of AI: automated malware adapting and spreading within minutes, credential theft campaigns targeting hybrid users at scale, and AI-powered phishing lures bypassing traditional email filters.

The old way of managing cybersecurity, manual threat hunting, reactive incident response, and siloed tools, simply cannot keep up. To survive, security operations must evolve from slow, human-centered models to machine-speed defense systems with humans in the loop.

Cybersecurity automation is not about replacing human analysts, it's a way to scale their reach. This means integrating intelligence, detection, and response across the full security stack, allowing:

- Real-time threat detection without manual log analysis.
- Automated response actions, like isolating infected devices instantly.
- Adaptive policy enforcement and continuous compliance checks without manual audits.

"

$2.22 million higher breach costs for companies without security automation.

IBM's 2024 Cost of a Data Breach Report. The longer threats stay undetected, the more expensive the fallout becomes.

OLD WAY VS. NEW WAY

A quick example

Imagine a mid-sized enterprise. A phishing email bypasses basic filters and steals a user's VPN credentials.

MANUAL SECURITY OPERATIONS

The security team detects unusual activity days later through manual log audits.

By the time the breach is identified, attackers have accessed confidential customer data in cloud services.

Response requires shutting down services, disclosing the breach, and absorbing legal and regulatory penalties.

AUTOMATED SECURITY OPERATIONS

An AI-driven behavioral analytics engine detects an impossible login sequence within minutes.

The system automatically revokes the compromised credentials and isolates affected endpoints.

An incident ticket captures full context and forensics begins immediately, no breach disclosure necessary.

In the manual case, the company faces major financial and reputational damage. In the automated case, the threat is neutralized before it becomes a crisis. Which option would you prefer?

CYBERSECURITY AUTOMATION

Key components of cybersecurity automation

COMPONENT	PURPOSE
Threat intelligence feeds	Update protections against new threats in real time.
Behavioral analysis engines	Detect anomalies like impossible travel logins or unusual data transfers.
Automated playbooks	Orchestrate step-by-step responses without human bottlenecks.
Dynamic access controls	Adjust user and device privileges automatically based on risk signals.
SIEM and SOAR integration	Consolidate detection, investigation, and response under a single pane of glass.

The goal is not "hands-off security." Work toward hands-smart security, where machines handle the noise and humans focus on strategy.

WHAT IT CANNOT DO

Context, customization, and oversight all matter: not every alert should be actioned without review, and humans must keep tuning automation to avoid blind spots.

BUILDING YOUR ROADMAP

Checklists and best practices

Migrating to a SASE, AI-driven, and automated security architecture is not a switch you flip. It's a phased journey requiring planning, executive sponsorship, realistic timelines, and a dash of patience.

Companies that treat this as a technology refresh usually struggle to generate long-term value. Companies that treat it as a strategic transformation usually succeed. The goal of the next chapter is to map out what a realistic transformation timeline looks like, including:

- Expected challenges
- Milestones to track
- Practical success metrics

A REALISTIC TRANSFORMATION TIMELINE

A realistic SASE and AI transformation timeline

Implementing SASE doesn't happen overnight. Here's a typical timeline across two phases, so you know what to expect.

PHASE 1 Foundation and planning

Application inventory: map critical apps, data flows, and user access patterns.

Security posture assessment: identify gaps across cloud and on-prem.

Select initial vendors: prioritize solutions that integrate into existing identity and security models.

Build the business case: tie the project to risk reduction, savings, and compliance.

COMMON CHALLENGES

Internal resistance to change, budget pressure from overlapping systems, and translating old policies into identity-based frameworks.

PHASE 2 Early implementation and validation

Deploy SASE for a pilot group: choose low-risk, high-value user groups or sites.

Begin unified policy rollout: start with web traffic, SaaS access, and identity-based enforcement.

Introduce AI-driven operations gradually: start with telemetry ingestion and baseline anomaly detection.

Implement basic automation: automate incident ticketing and basic device isolation.

COMMON CHALLENGES

Increased help desk traffic, managing hybrid operations, and fine-tuning AI thresholds to reduce false positives.

WHAT'S NEXT

Turning automation into your competitive advantage

Laying the foundation is step one. Adding automation and AI to reduce complexity and accelerate decisions is step two. But turning this into a long-term, scalable advantage requires a plan and a realistic understanding of how transformation unfolds over time.

The shift to intelligent operations reduces overhead and improves response times. More importantly, it allows IT teams to move at the speed of the business. With a modern foundation in place, enterprises can replace manual processes with automated workflows, use AI to surface insights before problems escalate, and respond to threats in real time. These aren't future-state ideas, they're already delivering measurable impact.

But sustaining that progress takes more than tools: deliberate planning, long-term optimization, and a commitment to continuous improvement.

WHAT'S NEXT

eBook three unpacks how to evolve your environment over time, scale securely, and build lasting resilience across every layer of your infrastructure.

MOMENTUM
EMEA

READY TO GET STARTED?

Book a call to learn how you can lay the foundation for AI-powered security.

Momentum's portfolio of SD-WAN and SASE solutions helps enterprises move from reactive operations to intelligent, automated, machine-speed defense.

Book a call

MOMENTUM EMEA

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