AI for networking
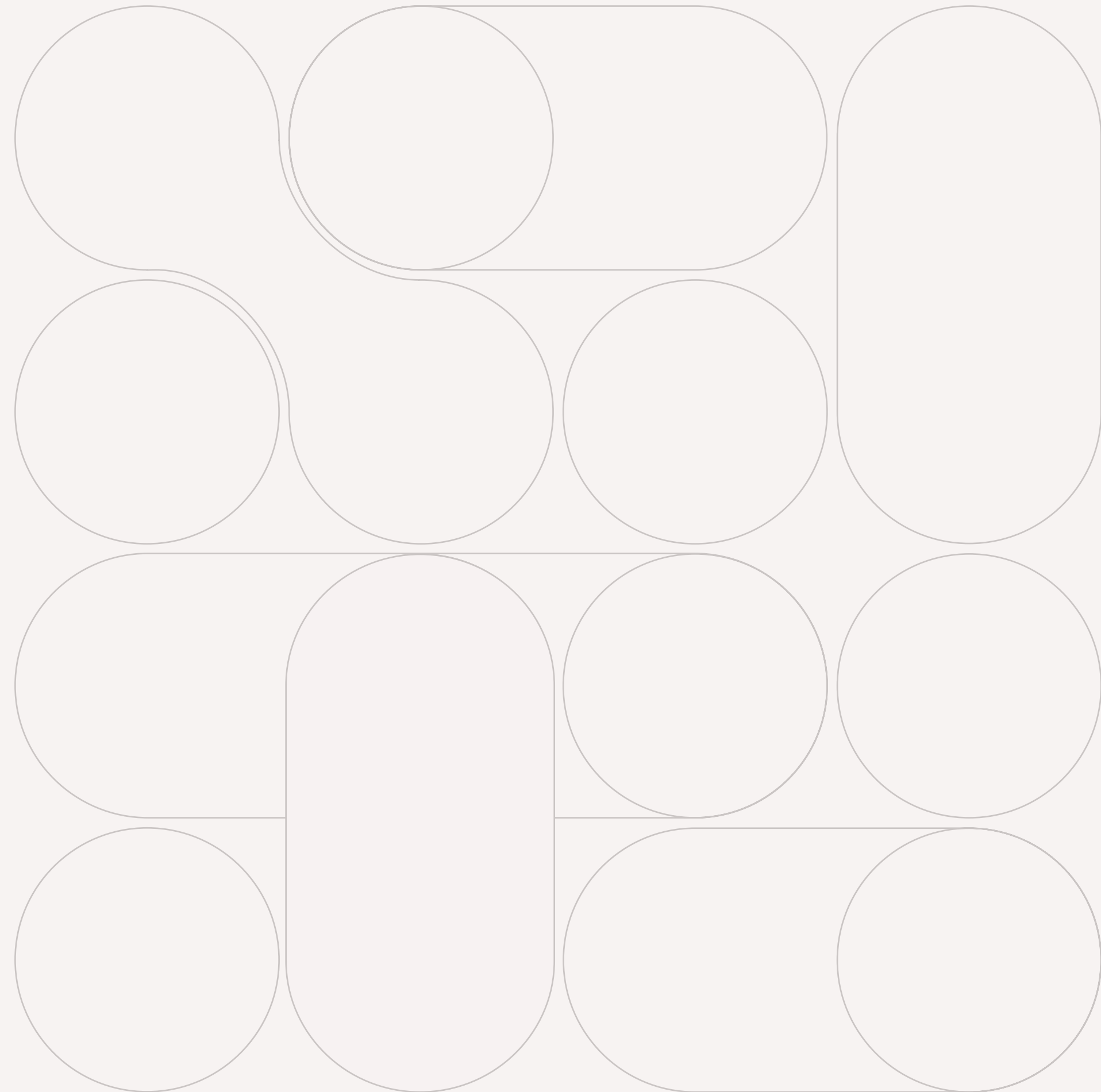
Beyond automation: Building self-healing networks with purpose-built AI

IBM

Contents

01

Why purpose-built AI for networks?

To say that modern networks are complex is an understatement. Large, dynamic and deeply distributed, today's networks are a labyrinth of legacy infrastructure, cloud-native systems and 5G deployments—with interconnected servic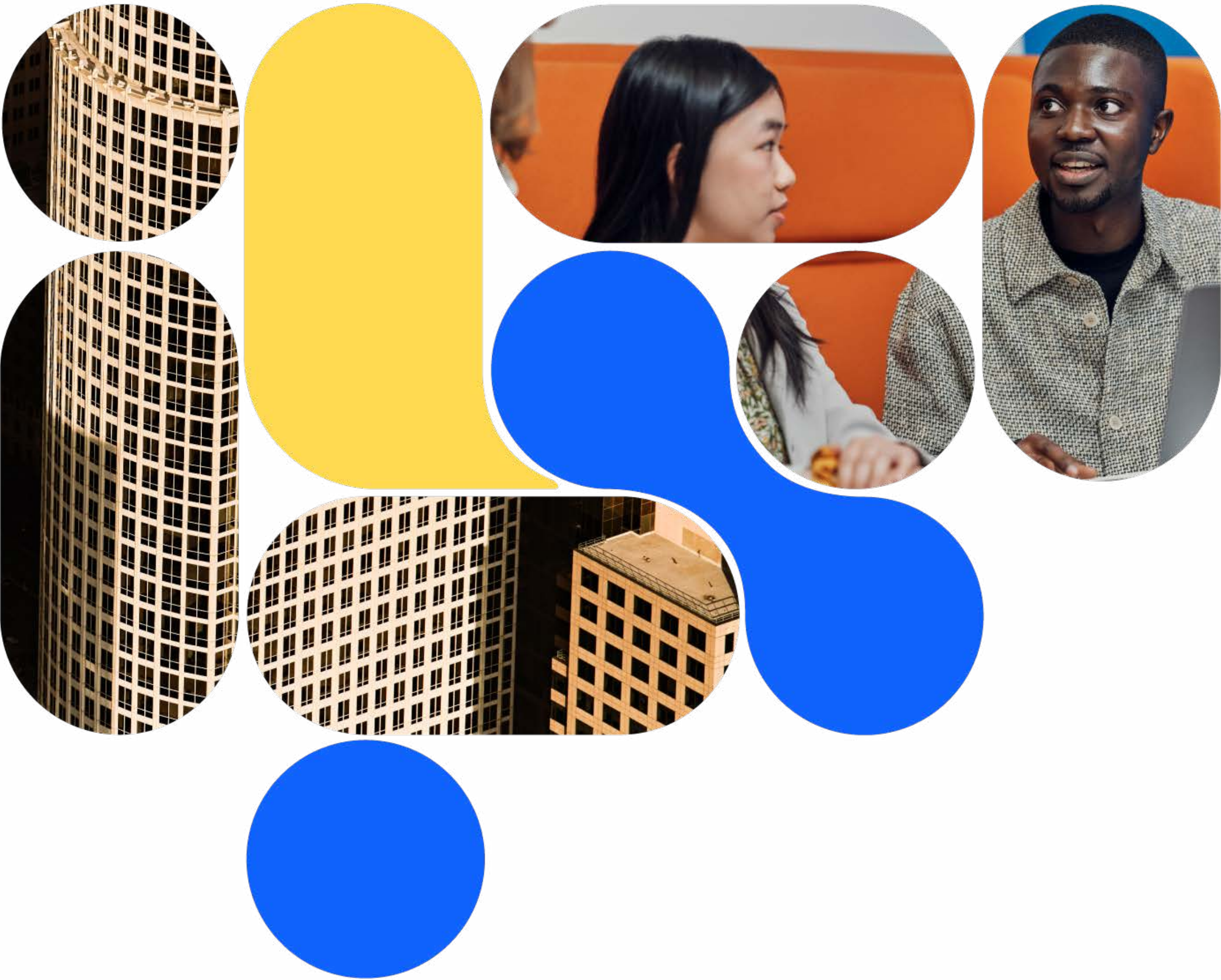e dependencies. According to a report by Broadcom, 78% of organizations surveyed stated that network complexity has grown significantly over the last few years.[1]

Network operations teams have the unenviable task of managing all this complexity. The greater the complexity, the higher the operational risks: new security vulnerabilities, false positives, slow root cause analysis, lower network visibility, rising operating expenses and more. There's also the possibility of potential anomalies going undetected, which can lead to network slowdowns and prove costly for businesses.

Networks generate huge volumes of data every second. Data that's siloed, complex and highly fragmented, impacting network visibility, slowing response times and blocking autonomous operations. To harness the potential of AI, organizations must provide the right data, but security and sovereignty concerns often limit access. Network engineers are left to navigate the maze of data and identify issues in real time, which is virtually impossible.

Unified data capture and analysis is one of the biggest challenges network engineers face today. As the network sprawl increases and endpoints multiply, it becomes harder to get a unified observability experience across legacy infrastructure, new systems and multiple networking domains. It's a case of too much data but too few insights. For network teams, this means that key issues are missed and response times are longer when incidents occur. The scale and complexity of modern networks also lead to an explosion of ticket volumes. Without timely operational insights, filtering out false positives and prioritizing issues that truly matter turn into an uphill battle.

Network engineers have been using traditional tools to address operational risks and maintain performance. While these tools—some even enhanced with generic AI—offer automated or semi-automated capabilities to improve operational efficiency, organizations are starting to see the limits of what automation alone can do. The fact is that basic automation can fall short in solving systemic issues, such as siloed datasets, cross-domain analysis and network lifecycle management. Automation also creates new challenges with maintenance, version control and signal overload.

As network operators face increasing pressure to do more with less, working with data silos and reactive workflows can seriously limit their efficiency. Bringing down OpEx is a key challenge for any network team. One way to do this is to reduce the amount of time spent on incident lifecycle management, which in turn lowers operational costs. However, network operators are bogged down by too many tools and a high rate of false positives, leading to a considerable drain on OpEx. To achieve next-level NetOps efficiencies, network teams need to go beyond just detecting and reacting to incidents; they should be able to forecast, adapt and resolve issues in near real time. And this is where AI comes in.
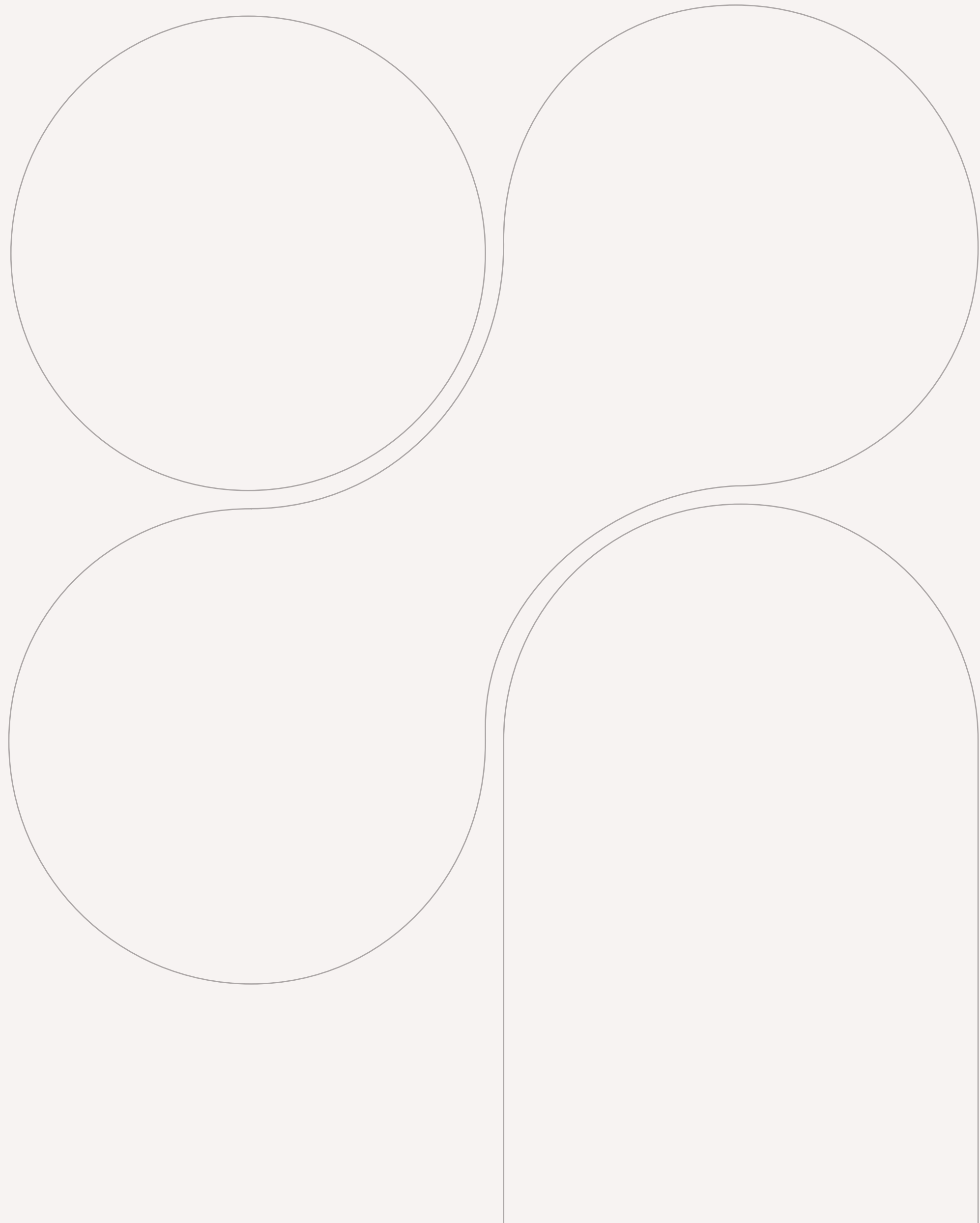
AI-driven network operations bring advanced monitoring and security, predictive capabilities, adaptive control and greater scalability, transforming network management from static and reactive to dynamic and proactive. However, just slapping generic AI onto network management tools won't cut it. Networks are driven by time series data. Generic large language models (LLMs) can't process such data, which can lead to misdiagnosed data and unreliable results. Networks need AI that's purpose-built—using specialized LLMs that can understand network-specific data and deliver trustworthy output. In short, a network management solution that's built with network-native AI.

Networks are driven → by time series data.

Generic large language models can't process such data and could generate unreliable results. This is why networks need AI that's purpose-built.
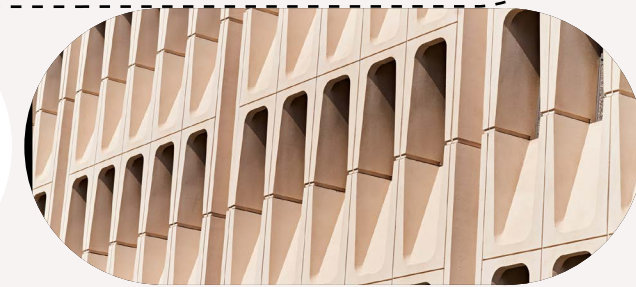
02

Overcoming the roadblocks to autonomy in modern network management

Today's networks are intelligent, dynamic and scalable multi-vendor environments designed to meet the demands of the digital business landscape. These systems need high levels of operational agility, which traditional network management cannot keep up with. Old techniques and approaches, such as rules-based management and threshold-based management, have proven inefficient in modern software-defined environments. And traditional tools, at best, are only capable of monitoring these environments, not managing network behaviors in real time. To keep pace with fast-changing business demands, network engineers need a scalable way to cut through false positives, root cause ambiguity and operational silos and get to the insights they require to run operations efficiently.

The changing landscape of network management: From reactive to proactive and autonomous

Network slowdowns. Outages. Security breaches. For too long, organizations have had to deal with these issues after the fact when network management was reactive in nature, resulting in higher operational costs and unplanned downtime. But today, no business can afford such interruptions. Consequently, network management has evolved from its firefighting mindset, adopting a more preventive approach to anticipate and act on incidents before they turn into issues. Network automation has further improved efficiencies by taking over repetitive tasks, reducing manual effort and speeding up response.
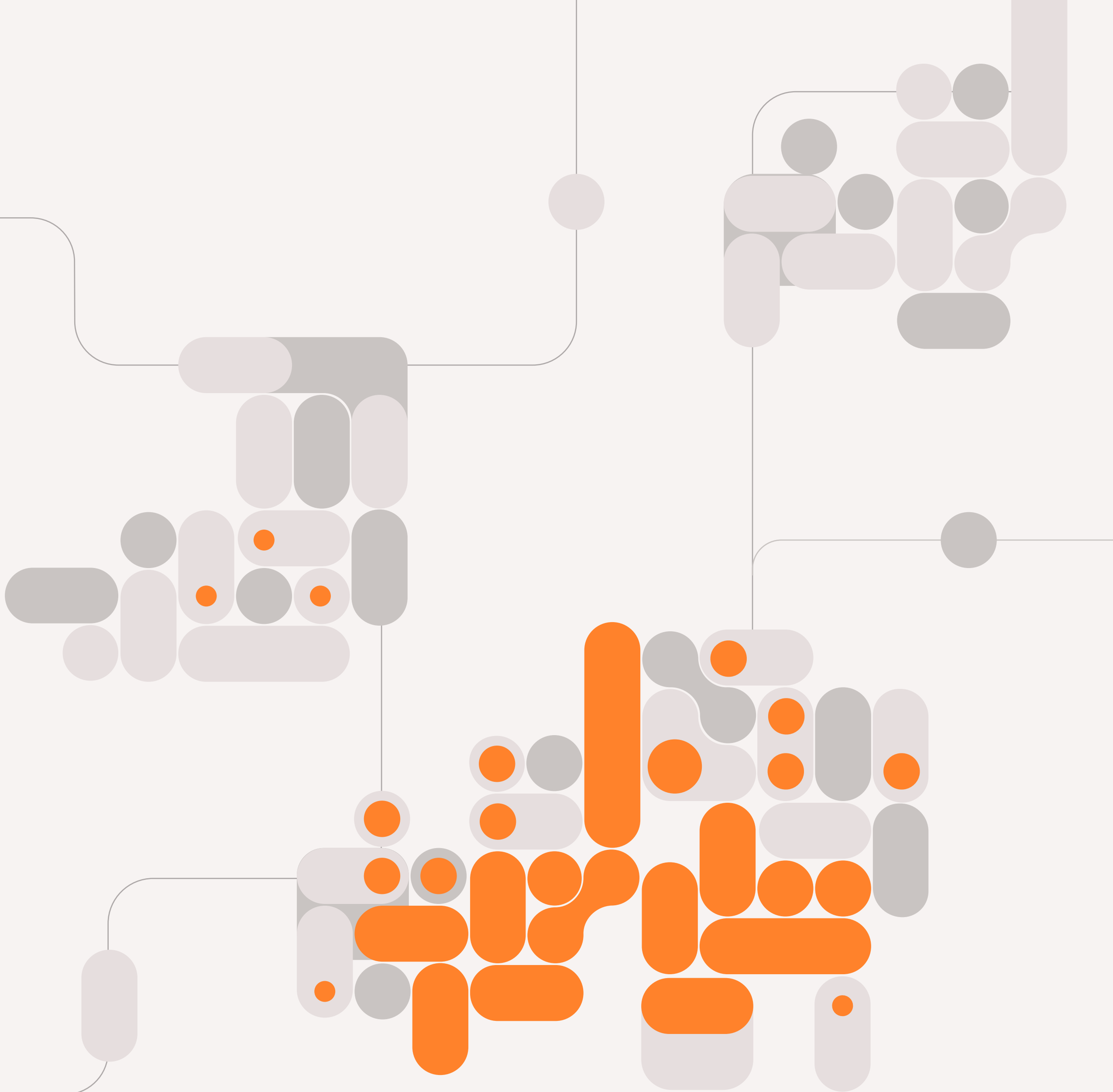
Overcoming the roadblocks to autonomy in modern network management

As networks grow more complex and business demands surge, true network autonomy is being looked upon as the logical next step in this evolution. Organizations now need networks that fix themselves, by autonomously identifying and remediating issues before they impact business—while keeping humans in the loop for validation and building trust. The shift toward autonomous network operations is inevitable. However, most organizations are still behind the curve on AI and autonomy.

Self-healing network technology has been around since the early 2000s. A self-healing network understands intent, validates and adjusts configurations, and adapts to traffic patterns and operational feedback to ensure reliability and performance at scale. But until recently, this approach has been adopted only in very specific areas and in controlled environments where trust has already been established. In modern networks, which are inherently more programmable than the networks of the past, the hesitancy to allow self-configuration and self-healing has more to do with the complexities of distributed systems. There's just too much that could break. So, embedding autonomy across the full network lifecycle has been unattainable for most organizations.

There are three key factors that make organizations reluctant to adopt AI-driven network autonomy:
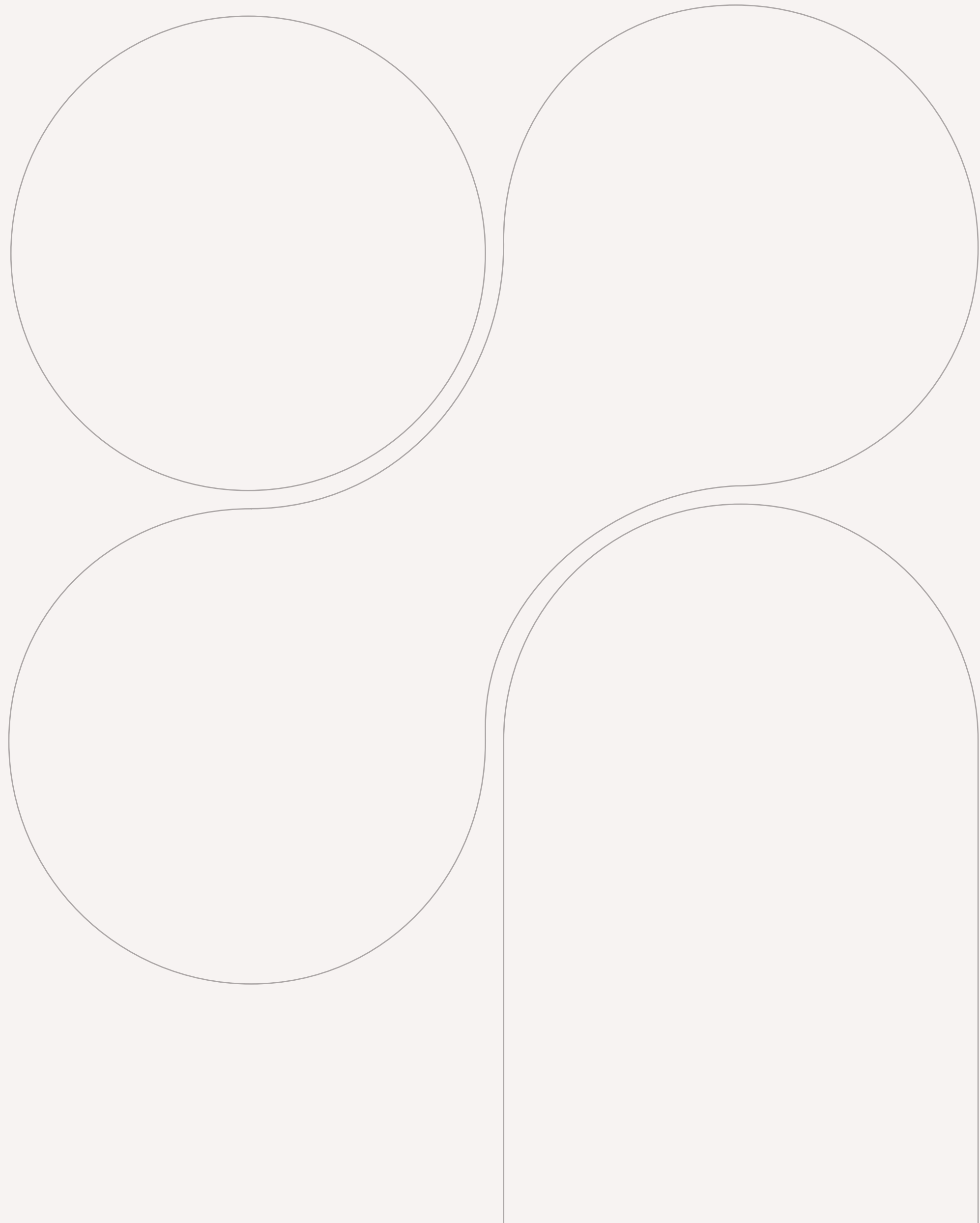
– Lack of confidence: Most businesses haven't seen the evidence that AI-driven autonomy can manage business-critical systems at scale. Network teams lack trust in *black box* systems that make decisions without clear explanations.
– Data issues: Data fragmentation across multiple domains, vendors and legacy systems hinders the availability of unified, cross-domain data that AI requires to deliver meaningful value in complex network environments.
– Skills gap: Businesses face a critical shortage of professionals with the deep networking expertise and AI capabilities needed to build and integrate autonomous systems across an ever-shifting network landscape.

From static automation to intelligent autonomy

Making the transition toward autonomy requires an approach that builds confidence in network insights every step of the way. An approach that supercharges—not replaces—your existing network systems, helping you act faster, resolve smarter and adopt autonomous actions at the pace you set. It's a journey that you can start by introducing AI into your day-to-day network operations to deliver quick, achievable wins such as:

Reduced ticket noise
Focus network teams on tickets that matter, with fewer false positives

Data visibility across silos
Bring scattered datasets together to generate the right insights

Faster action
Translate data into meaningful action with less operational overhead

Explainable insights
Provide context-rich responses that are traceable and verifiable

Consistent, explainable outcomes delivered over time can help you build the confidence necessary to gradually ease humans out of the loop of routine tasks toward a more supervisory role. As you rely more on autonomous operations, you can expand the scope to include new data domains and enable cross-domain analysis that will eventually help you complete the data picture. This carefully considered, step-by-step process is a more realistic path toward network autonomy. And more importantly, it's a journey that can be made possible only with AI that's purpose-built for networks.

03

A new era of intelligent network automation powered by agentic AI

Network complexity cannot be wished away.
Organizations have to find a way to move
from complexity to clarity by making sense of
all their network data—however fragmented
it is—and acting on it. For network leaders,
the tasks at hand are many.

– Accelerate time to diagnosis
– Reduce false positives with
  contextual correlation
– Minimize operational costs
  and unplanned downtime
– Extend mean time between
  incidents (MTBI) and reduce
  mean time to repair (MTTR)

To reduce repeat incidents and resolve
issues faster—without increasing
headcount—network teams need efficient
root cause analysis and AI they can trust.
Transparent decision-making, safety
guardrails and clear explanations help
teams understand why actions were taken,
building confidence in the system.

That's why network-native AI is essential. It delivers actionable insights that enhance performance, reliability and security, while minimizing operational costs and downtime—without the need for second-guessing.

→ Nearly two in three telecom executives say autonomous networks can enable new service models and drive revenue growth.[2]

Introducing IBM Network Intelligence

IBM® Network Intelligence can accelerate your shift to autonomous network operations with agentic AI-driven, cross-domain actions across multi-vendor and multi-domain environments. Built on IBM's domain-trained time series foundation models and agentic AI reasoning, the solution is designed to redefine network operations and deliver explainable insights, guided automation and closed-loop actions. Whether you are looking to reduce MTTR, extend MTBI or cut operational noise, this solution is built to be your frontline intelligence for always-on, always-evolving networks.

A new era of intelligent network automation powered by agentic AI

Purpose-built for multi-vendor environments, IBM Network Intelligence ingests and analyzes data across domains, filters out false positives and identifies root causes using agentic AI—to help you navigate network complexity with enhanced clarity and speed. At its core is a multi-model architecture with semantic context for domain awareness. The solution combines precise root cause insights with semantic understanding to generate prescriptive plans that balance logic and context, enabling AI agents to drive toward autonomous action. With built-in integrations across multi-vendor environments, domains and automation platforms, IBM Network Intelligence helps you stay in control while fast-tracking your journey to network autonomy.

With IBM Network Intelligence, you can add AI into the mix of your existing tools or NetOps. The solution is designed to enhance what you already have—aiming to bring intelligence, speed and clarity to every layer of your network. By triggering intelligent actions through your existing automation tools, the solution positions your team to resolve issues faster. From detection to resolution, IBM Network Intelligence helps you scale operations without necessarily increasing costs, accelerating your journey from manual troubleshooting to self-healing networks.

A new era of intelligent network automation powered by agentic AI
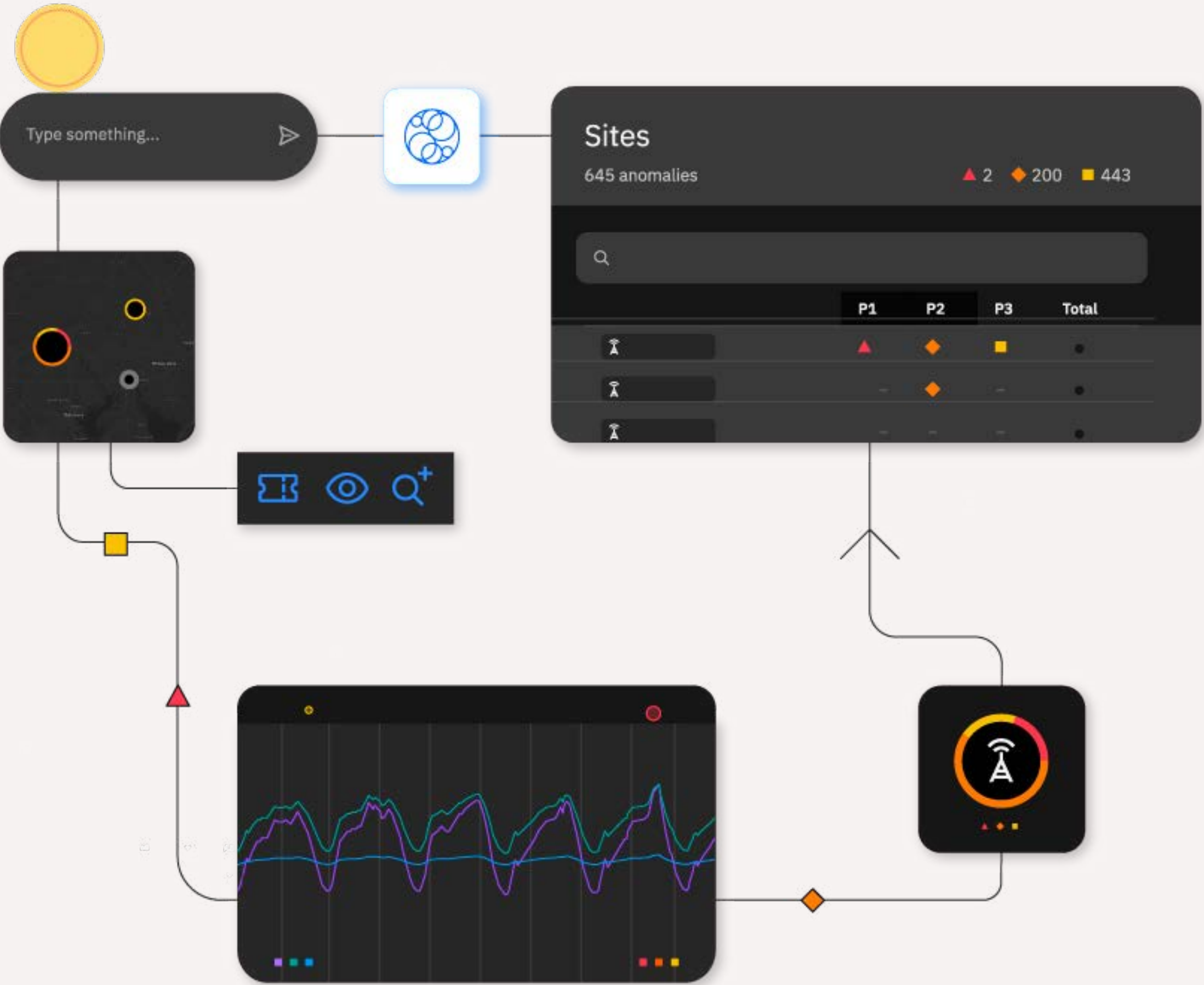
Key features and benefits
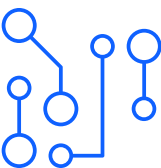
AI built for networks, not bolted on:
Experience deeper, more accurate insights with a purpose-built solution that features domain-trained time series models, agentic AI capabilities and embedded semantic intelligence to understand network-specific behavior. The models are trained on high-volume telemetry, alarms and configuration changes across diverse network environments, enabling deep contextual understanding and providing a path to intelligent automation at scale.
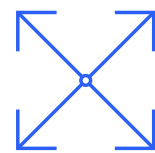
Fast time to value:
Get started quickly with off-the-shelf integration, a chatbot interface and a streaming data pipeline that are intended for continuous learning and adaptation. Take advantage of simple data ingestion that sits on top of existing data sources and ticketing systems, aimed at detecting service-impacting issues early with lower false positives. Achieve quick ROI through modular deployment, pre-trained domain-specific models—including time series foundation models—and rapid integration capabilities.
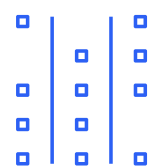
Interoperability and scalability:
Optimize operations with a solution designed to plug into any environment with an architecture that can work across network domains, vendors, solutions and deployment models. IBM Network Intelligence is engineered to scale with your network and adapt as your operations evolve. Built-in guardrails enable safer execution: if a plan exceeds a defined blast radius, the system prompts for user confirmation before proceeding. The solution also intelligently filters out non-network-related or out-of-scope requests.

Responsible AI for greater trust and faster adoption:
Equip your network with responsible AI that's positioned to reduce the risk of wrong decisions and minimize the effort required to correct mistakes made by AI. Through guardian models that protect against training and inference risks and design tweaks that improve user trust—with human in the loop at optimal decision points in the AI workflow—responsible AI is engineered to build trust and accelerate adoption.

A new era of intelligent network automation powered by agentic AI

End-to-end network lifecycle management:
Empower your team with a solution built to drive complete network lifecycle management, from planning to performance optimization. Experience how it's structured to achieve continuous alignment between network health and evolving business priorities by integrating what's often fragmented across teams, tools and data sources.

Unified network operations:
Drive efficient operations with a solution designed to utilize multi-vendor and multi-domain support across Cisco, Juniper, Nokia, cloud solutions, leading data lakes, network observability tools, software-defined stacks and vendor APIs. Ingest and analyze logs from multiple network systems and generate insights—without disrupting your current systems.

Automated remediation:
Identify issues quickly with a solution engineered to reduce the signal-to-noise ratio and feed insights automatically into remediation pipelines using pre-built or custom data integrations. Gradually adopt agent-driven actions and move toward autonomy at your own pace.
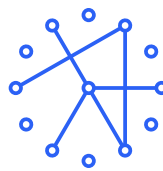
Network optimization:
Go beyond insights with agentic AI that learns, reasons and acts—to create tickets or remediate issues. See the AI evolve along with your network, with intelligent self-healing capabilities that help optimize network operations.
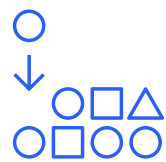
OpEx in control:
Automate routine tasks, provide intelligent insights and enable agentic problem-solving to help drive network growth without a proportional increase in operational costs.

Built to make you proactive, not reactive

IBM Network Intelligence empowers stakeholders with role-based, cross-domain intelligence. The result? A path to improved reliability, reduced costs and extended MTBI while transitioning from automation to autonomy—with fewer disruptions to your network.

A new era of intelligent network automation powered by agentic AI
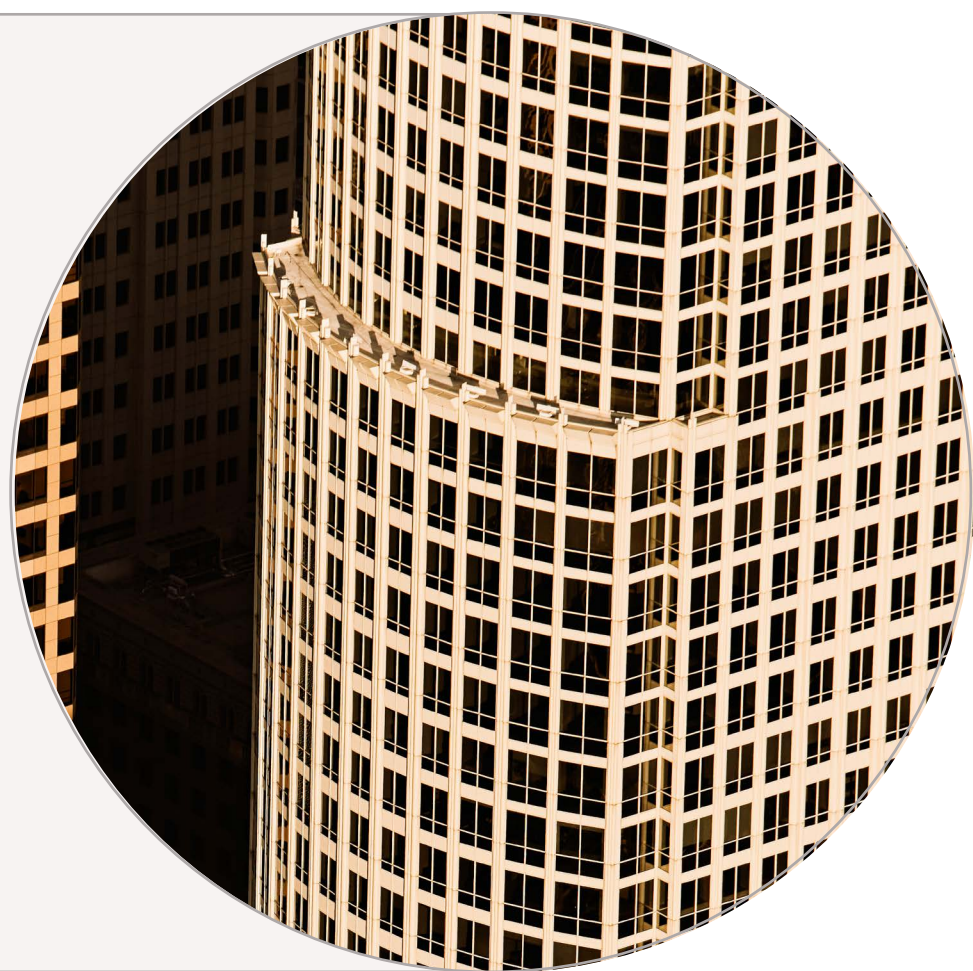
How can stakeholders benefit?

Network operations leaders:
IBM Network Intelligence is built to deliver autonomy—without the chaos. It can unify your stack, slash false positives and boost MTBI. Unlike other solutions, IBM Network Intelligence plugs right into your existing environment—less rework, less disruption. With intelligent root cause detection and cross-domain insights, your NetOps teams can work faster, your costs can drop, and your network can scale on your terms.
It's not just another solution; it's a path to smarter, autonomous network operations. Built for today. Ready for what's next.

Practitioners:
IBM Network Intelligence, powered by agentic AI, proactively surfaces issues without waiting for you to ask. It observes behavior across domains, maps dependencies and tells you what broke, why it happened and how you can fix it—before you even start looking. No rules to configure. No dashboards to dig through. Just fast, explainable answers—you can thank it later. Built for practitioners who don't have time to drown in false positives or sort signal from noise. This is root cause analysis reimagined for high-stakes environments—where uptime isn't a goal, it's the baseline.

04

Infusing AI across the complete network lifecycle management

Are you looking to modernize NetOps? Or are you preparing for full automation? No matter where you are on your network automation journey, IBM Network Intelligence can meet you where you are and get you where you need to be. From making network management more efficient to laying the groundwork for intelligent network operations, the solution helps map and progress your journey to an autonomous future.

The closed-loop system: Embedding intelligence across the network lifecycle
How do you extend intelligence across your entire network lifecycle? IBM Network Intelligence takes a holistic view, right from planning and designing to building and operating—unlike other AIOps tools in the market that focus just on operations. The solution adopts a closed-loop approach to facilitate intelligent automation at every stage of the network lifecycle. The three stages— plan and design (Day 0), build and deploy (Day 1) and operate and assure (Day 2)—exist in a closed loop with insights and observations feeding back into the cycle to help drive continuous improvement and optimization.

How the closed-loop system works
Beginning with Day 2, which is daily operations, you add AI to your existing systems to handle mundane network tasks. As the AI learns to detect issues, surface probable causes and generate plans for optimization, you can expand its remit to include new domains and teams. While your existing instrumentation may not detect blind spots, such as recurring errors or emerging behaviors, AI can observe such slow degradations in performance early on and act proactively to help minimize downtime. With the power of semantic-aware deep learning and agentic AI, you can reduce manual workloads, extend MTBI and gradually enable resilient, self-healing network operations.

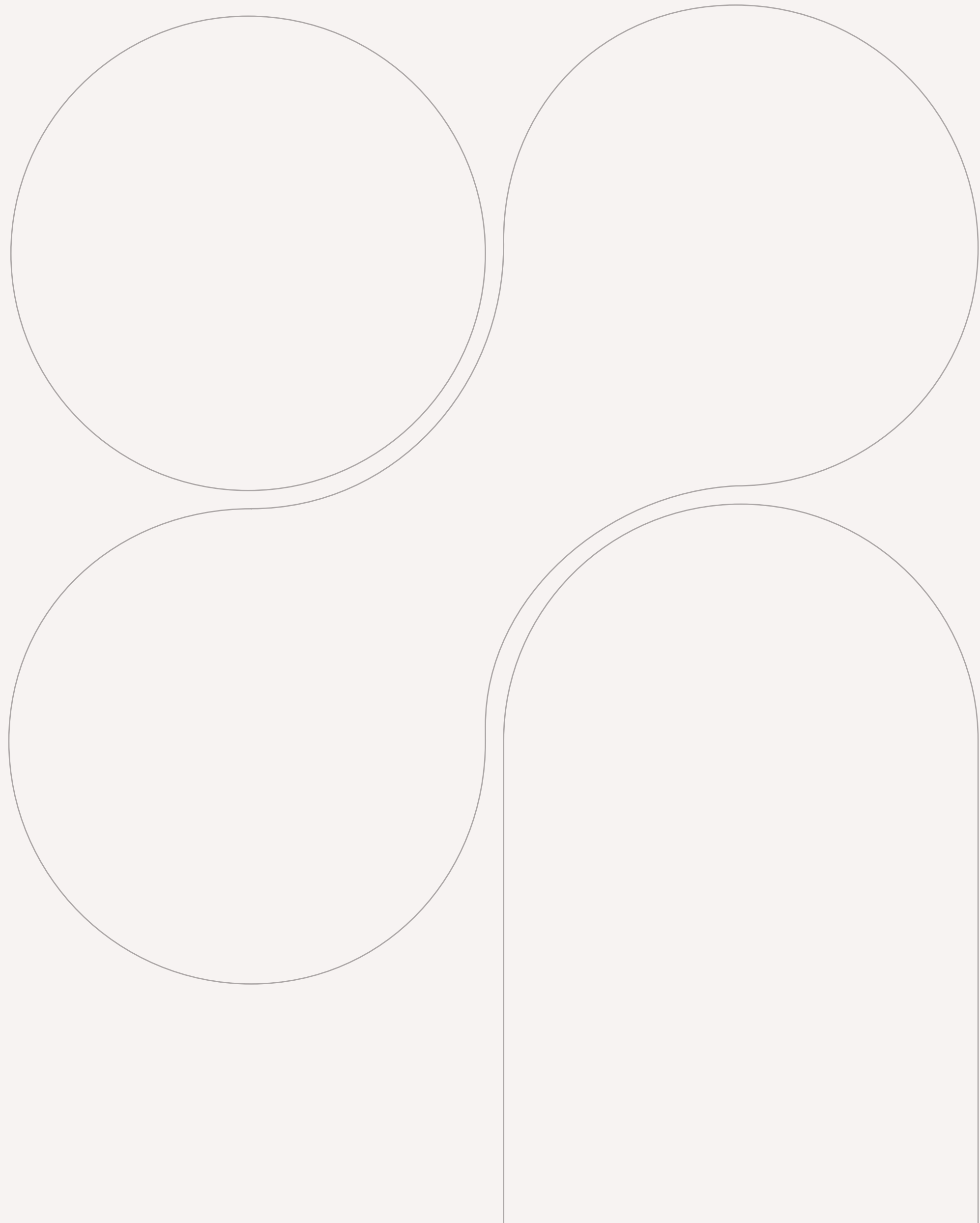Infusing AI across the complete network lifecycle management
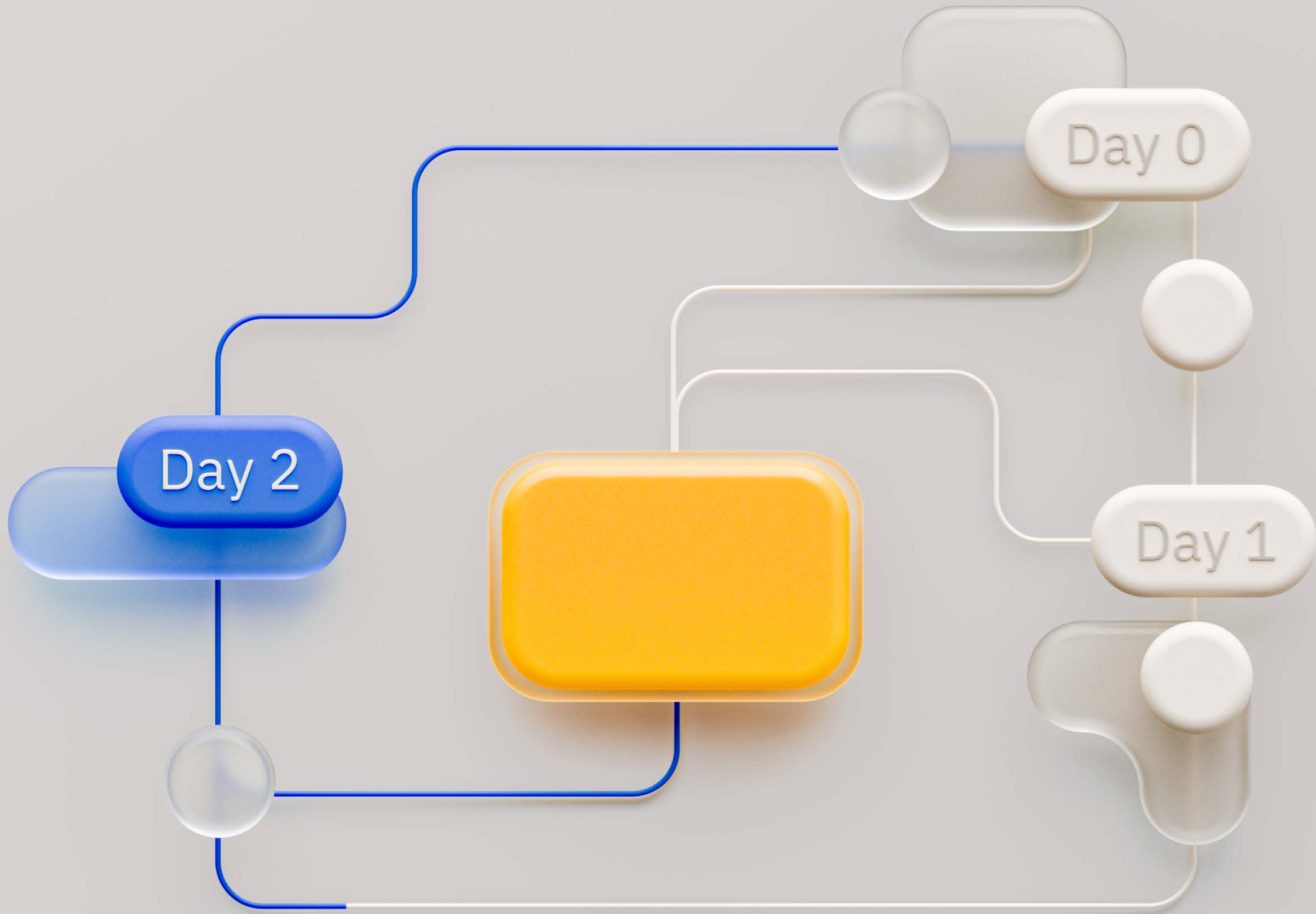
In the next phase, you move to Day 0 and Day 1, integrating AI into the plan and build stages of the network lifecycle. AI is built to accelerate strategic planning, design and modernization efforts by leveraging historical analytics, best-practice inference and intent-based service design. Using natural language inputs and graph-based models, you can automate network architecture generation to help reduce planning time. Intent-based design predicts future traffic demands, driving network optimizations to handle data growth and scale. Capabilities such as vendor swap simulation, coverage and capacity planning, and self-configuration help reduce design complexity.

In the build stage, AI can simplify and optimize resource allocation and service rollout to facilitate network feasibility validation and establish fallout management. The result could include reduced deployment times and errors, more efficient CapEx allocation and faster time to market.

The closed loop of observations, insights and refinement enables the AI to adapt and build trust in its outputs and actions, driving continuous network optimization and improved performance and efficiency.
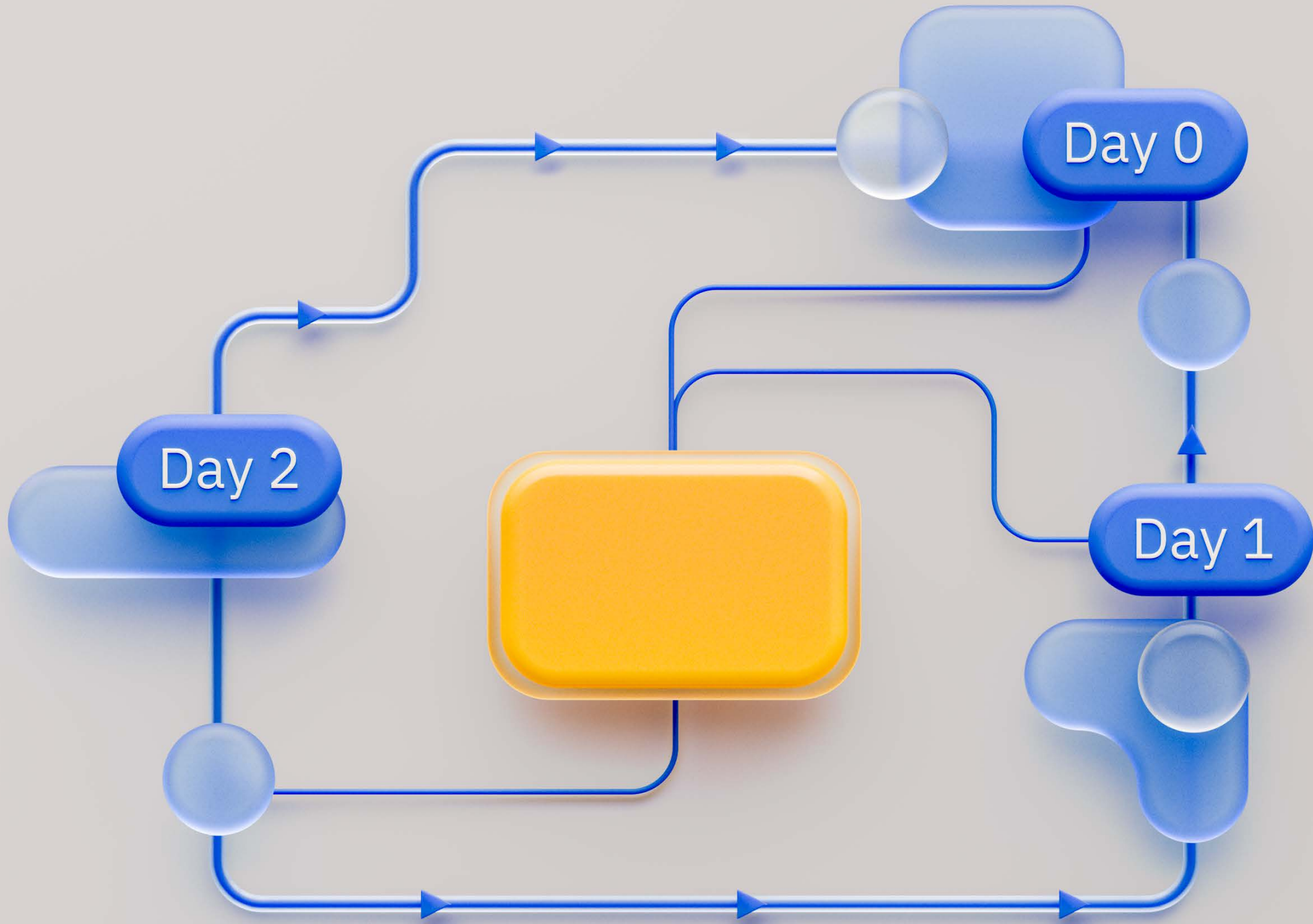
05

Network automation
in action

Example 1: Internet Protocol Multi-Protocol Label Switching (IP/MPLS) silent drops (Telco and Enterprise)

AI-powered network automation is bringing new levels of accuracy and reliability to operations, helping optimize utilization rates and resourcing, reduce operational costs, minimize downtime and make self-healing networks possible. Let's look at a key use case involving network issue lifecycle management and see how you can redefine it with IBM Network Intelligence through a few examples.

Detect silent failures and resolve root causes faster
Silent drops break critical enterprise flows—and no one knows until it's too late. IBM Network Intelligence uses agentic AI to detect issues other tools may miss, trace root causes across layers and help fix them quickly. You get clear visibility, fewer escalations and uninterrupted digital experiences—without digging through logs or juggling tools. From global backbones to enterprise wide-area networks (WANs), IBM Network Intelligence turns silent failure into silent recovery.
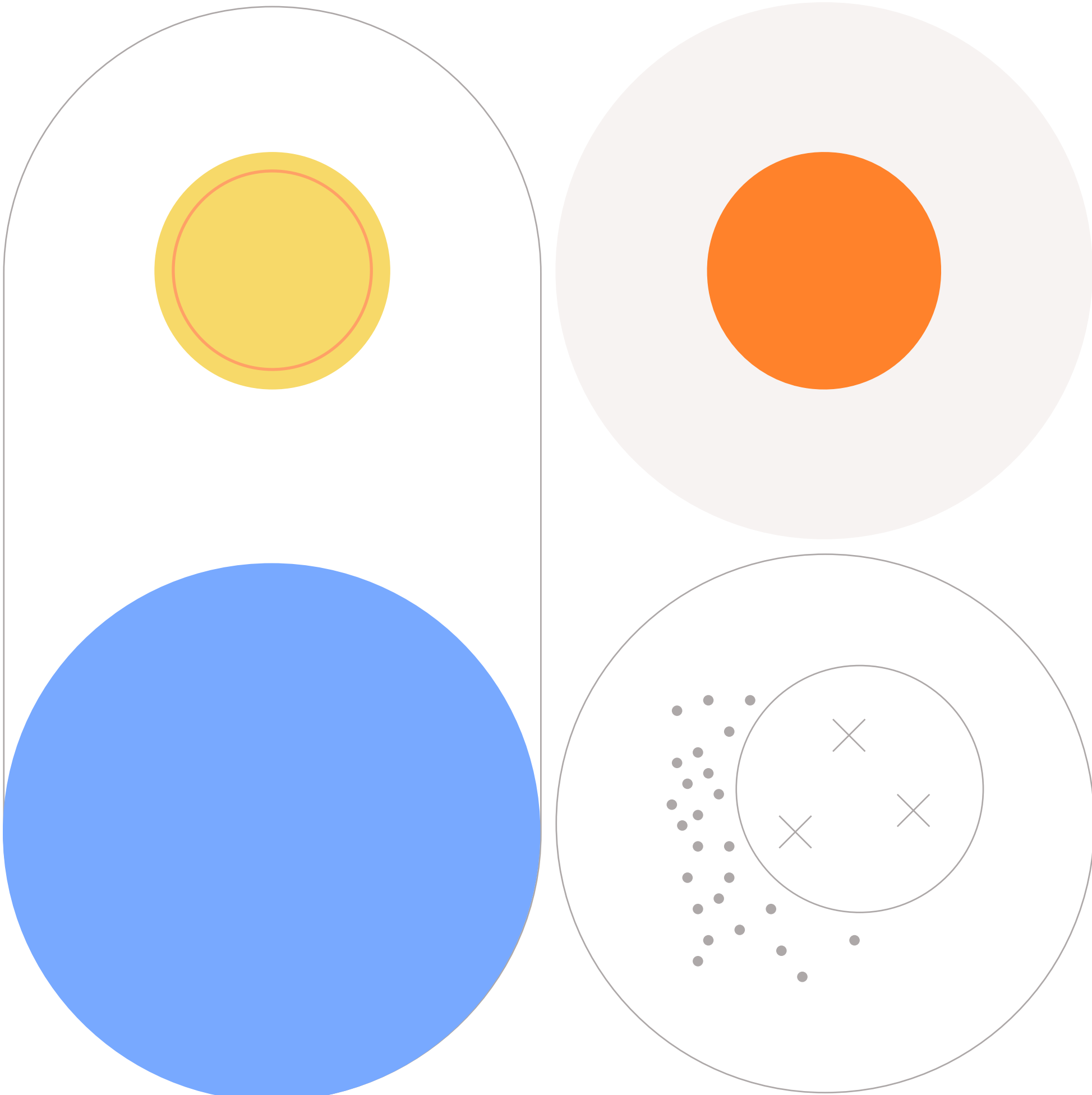
Example 2: Radio access network (RAN) domain optimization (Telco)

Automate RAN with agentic AI to fix congestion and boost experience
Congested cells? Dropped calls? Don't let RAN issues impact your experience or OpEx. IBM Network Intelligence brings autonomous intelligence to the radio domain—detecting congestion, interference and imbalance before customers even notice them. Agentic AI identifies root causes and acts immediately, tuning networks in near real time. No need to code or toggle between tools. Slash dropped calls, ease network operations center (NOC) fatigue and deliver consistent quality of experience (QoE) across urban and rural sites.
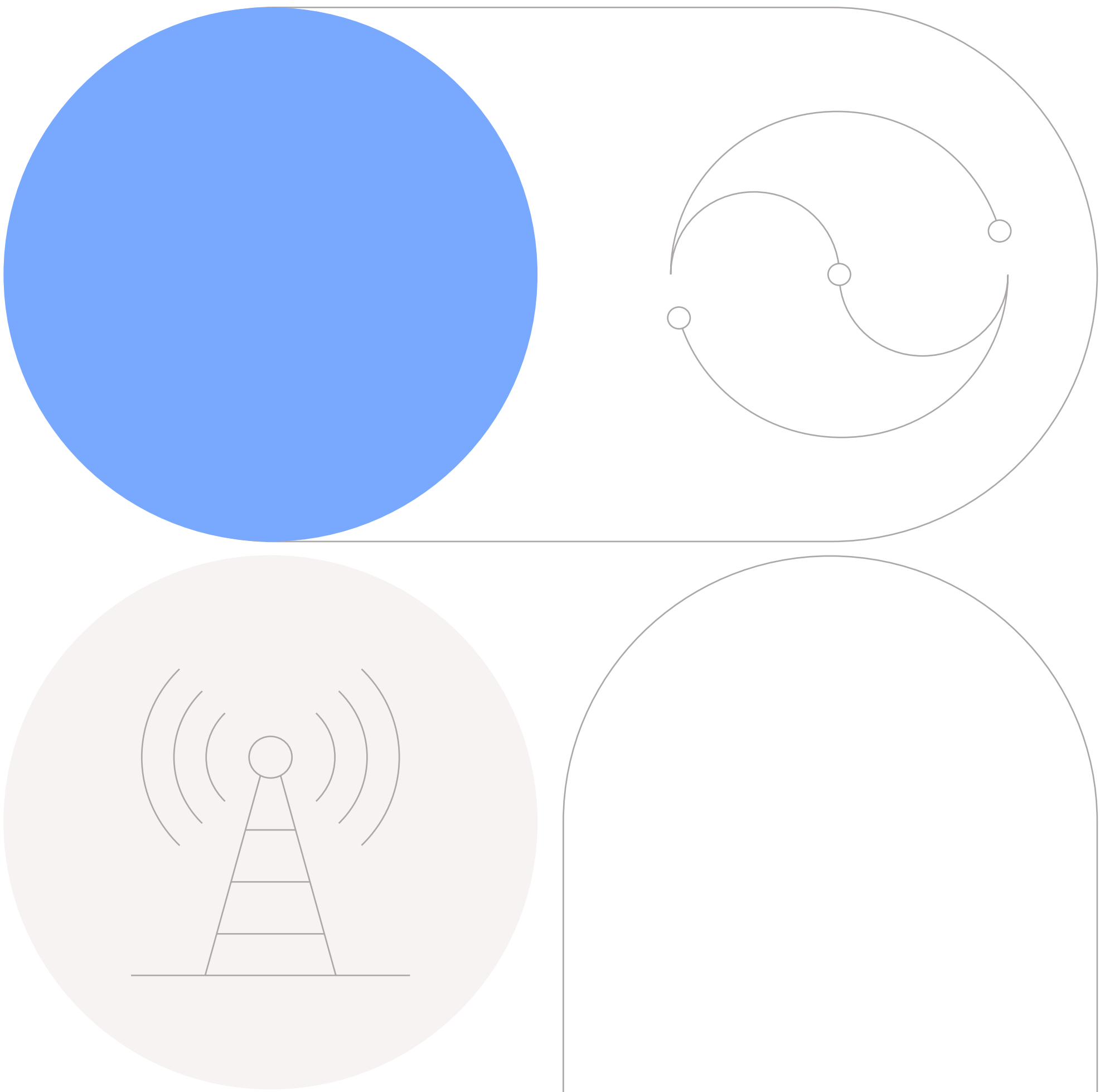
Example 3: Data center (DC) networks (Enterprise)

Power DCs that fix themselves with agentic AI—before impact hits
Data center complexity creates risk. IBM Network Intelligence brings agentic AI to detect slowdowns, path issues or misconfigurations before they cascade. It's designed to diagnose and fix problems fast—without code, chaos or disruption. You get more resilient, self-optimizing data centers that run smarter, can scale faster and stay one step ahead of failures. Build a self-healing foundation that's able to scale with business demands.

06
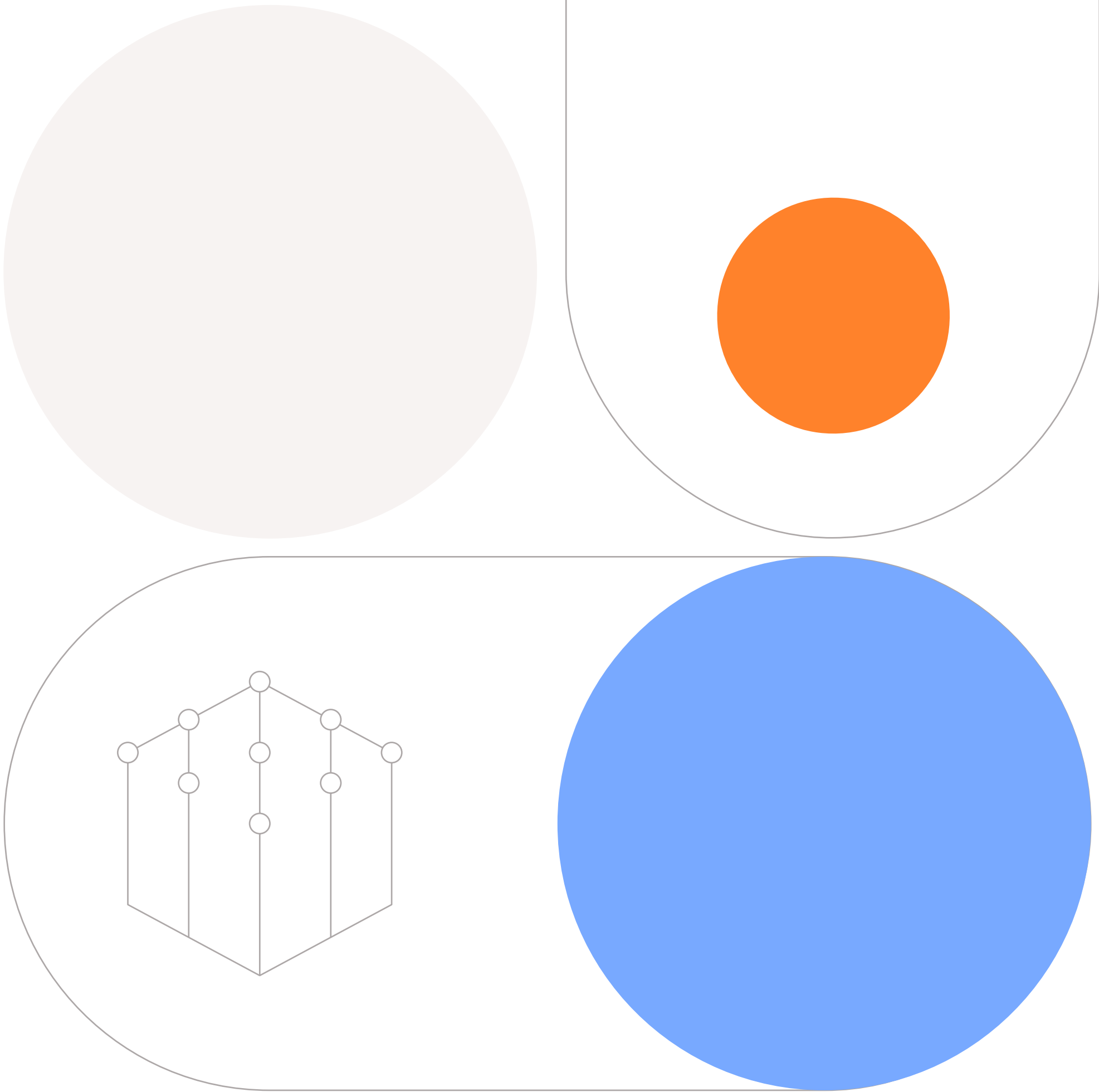
Why IBM?

Why IBM?

IBM meets your organization wherever you are in your automation journey. We can integrate our solution across your existing tools and environments to evolve operations and deliver actionable outcomes, not just insights. Unlike traditional network AI projects that take 6–8 months to train, tune and integrate, our solution provides faster results with prebuilt models and out-of-the-box capabilities.

We bring an independent perspective to resolving your operational challenges, working with leading networking vendors without favoring a specific vendor. We also have industry-leading tools, such as Ansible® and Terraform, which are probably already used by your enterprise.

With over 100 years of technology experience and proven leadership in enterprise AI, IBM is a technology partner you can trust to build responsible, network-native AI designed for true network autonomy.

Explore smarter networks in action. Learn more about how IBM Network Intelligence automates complex network tasks.

1. Cloud and Internet Usage Generates Network Observability Blind Spots, Broadcom, September 2024.

2. Navigating autonomous networks, IBM Institute for Business Value, 5 September 2025.