

A large, multi-colored arc (blue, purple, pink, orange) curves from the top left towards the bottom right, framing the main title text.

Run Lean: Turning Operational Simplicity into Compounding Value

A Phased Blueprint for Modernizing Infrastructure and Operations Without Paying the Fragmentation Tax

*For CIOs and IT Directors of growing
SMB & MM organizations*

How to read this paper: This blueprint is architecture-first and vendor-neutral. Each phase opens with the capability you need and **what to look for in any solution**, then a clearly marked **Cisco recommendation** for teams who want a single integrated operating plane. If you run mixed or non-Cisco infrastructure today, the phases still apply: adopt the operating model, keep what works, and treat the Cisco sections as one fully integrated way to deliver it.

Executive Summary

The mandate for 2026 is efficiency. Gartner's research puts productivity and cost optimization at the center of the CIO agenda, and more than half of CIOs say reducing costs will become an even more important objective over the next two years. The same research is blunt about the trap: cost-cutting that erodes capability is a short-term loss. The goal is to reposition cost as a strategic capability that funds growth.

Yet the lean IT teams expected to deliver that efficiency are quietly paying a **fragmentation tax**: the hidden, compounding cost of running the business across disconnected consoles, tools, and vendors. It never appears as a line item. It hides in the swivel-chair troubleshooting, the spreadsheet that reconciles two dashboards, the specialist you must hire per console, and the truck roll to stand up one more site. Each point tool looks affordable on its own. The tax lives in the gaps between them.

Adding another best-of-breed tool deepens the tax. Blunt cost-cutting erodes the capability you need. This paper presents the third path: invert the tax. Consolidate onto one operating plane where every capability you add **compounds the value** of the whole. Fewer consoles, more automation, and AI that gets smarter as telemetry accumulates.

The blueprint runs in four phases:

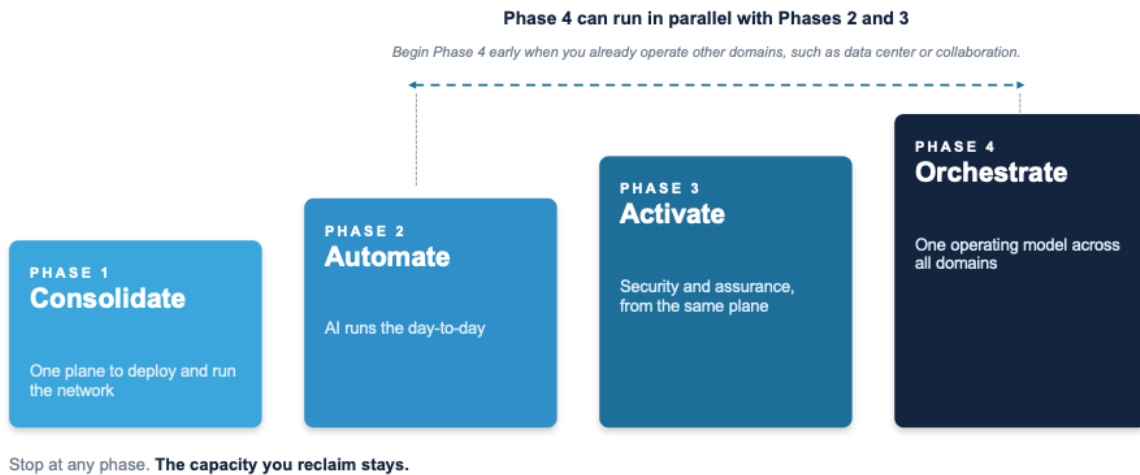
1. **Consolidate.** Bring at least one network component onto an unified cloud-managed plane, starting with whichever domain you are refreshing first.
2. **Automate.** Let AI and low-code automation run the day-to-day, so the team resolves issues faster and provisions without scripting. Continue to expand the network footprint based on your refresh cycle.
3. **Activate.** Light up advanced security and assurance features from the same plane. Zero-trust access, network micro-segmentation and deep-path monitoring are key pillars of a resilient network.
4. **Orchestrate.** Extend the unified estate to collaboration, data center, compute observability and data fabric while letting AI agents handle routine operations, with humans approving consequential change.

Note that phase 4 can run parallel with Phases 2 and 3, depending on your existing assets, expansion plans, and availability of a single operating platform.

The architectural idea in one line: **a fragmented estate compounds cost; one operating plane compounds value.**

Run Lean: A Blueprint That Compounds

Each phase is independently valuable. Stop at any phase and keep the capacity you have reclaimed.



1. The Problem: A Lean Team Paying the Fragmentation Tax

Growing organizations are adopting technology at enterprise pace with a fraction of the staff. They run the leanest IT teams, per employee, of any segment, and they face the same modernization pressure as everyone else: aging hardware reaching end of life, on-premises controllers to retire, and new AI-era demands on the network.

The instinct is to solve each gap with a specialist tool. A console for wireless, another for switching, another for the WAN, another for access control, another for monitoring. Each is defensible in isolation. Together they create the fragmentation tax: the compounding penalty an organization pays when its operations run across a patchwork of systems that do not talk to each other. The cost is real and measurable, but it does not invoice. It surfaces as alert storms, duplicated effort, delayed resolution, and time lost moving between tools instead of solving problems.

The cost is now quantified. The May 2026 Freshworks Global Cost of Complexity Report, a survey of more than 9,000 mid-market IT professionals, found that mid-market companies lose an average of **25% of their AI budgets** to complexity overhead before realizing a single dollar of return. And the drain is not only budget. Observability research from EMA, corroborated by Cisco Splunk's own data, finds that maintaining disjointed tools can consume up to **30% of senior engineers' time**, while the context-switching between them adds significant delay to mean-time-to-resolution during critical outages. This is the fragmentation tax made concrete: budget lost before value, and senior talent spent on tool-tending instead of the business.

For a lean team, this tax is existential. Every additional console is another integration to maintain, another skill set to staff, and another place the operational picture breaks.

Modernization that simply layers new tools on top of old ones makes the problem worse, not better.

Why the obvious fixes fail. The first reflex, buy the best tool for each job, is what created the fragmentation in the first place; more best-of-breed means more gaps. The second reflex, cut costs across the board, is the one Gartner explicitly warns against: cuts that erode capability trade a one-time saving for a permanent loss of performance. Neither addresses the structural problem, which is the number of disconnected places the team has to operate.

2. The Core Insight: Compounding Value Is the Inverse of the Fragmentation Tax

If fragmentation compounds cost, consolidation can compound value. The control point is the management plane.

On one operating plane, each capability you add does more than its own job. It reduces the number of consoles the team runs. It enables automation that spans domains instead of stopping at a tool boundary. And it adds telemetry to a shared pool, which makes the plane's AI more capable at troubleshooting and operating everything else. The second domain is more valuable than the first, and the fifth is more valuable still. That is the opposite of the fragmentation tax, and it is the strategic case for a single plane over a basket of point tools.

This is why the holistic strategy in this paper is not "buy more." It is "consolidate the operating model." Every phase below is designed to compound: nothing is thrown away, and each addition raises the value of what came before.

A fair question: does consolidation mean lock-in? It is the right thing to ask, and the answer depends entirely on *what* you consolidate onto. The goal should not be a single vendor for every box on the floor. It should be a single operating model, and here breadth is the point that gets overlooked. Unified management of networking and security is now common; many platforms already offer that pairing, so it is no longer a differentiator on its own. The harder and more valuable test is how *wide* a set of domains a single plane truly spans: networking and security, but also collaboration, data center, compute, observability, and the shared data layer beneath them. The wider the span, the more of the fragmentation tax the plane actually removes. Consolidating the operating model is what reclaims capacity; consolidating onto one vendor is a separate, optional choice.

The second property to demand of any such platform is that it be open by design. Look for an operating model that integrates third-party tools and systems through native connectors and open standards such as the Model Context Protocol (MCP), rather than reaching only its own products. The real test is whether any system that exposes an API and an agentic interface can join the model, including non-Cisco identity, security, and observability tools. The condition for participating should be capability, not brand.

That openness is what separates an operating model from a cage. You choose an anchor for how the estate is run, while keeping standards-based interoperability and a place for best-of-breed where it earns one. The compounding value of standardizing further on one vendor, fewer

consoles still, richer shared telemetry, tighter native integration, is a bonus you can capture if you choose to. It is not a toll you must pay to participate.

Where Cisco fits. It is also fair to ask whether the vendor proposing this has solved its own fragmentation first, because a unified plane is only credible if the company behind it is not itself a stack of disconnected consoles. Cisco's answer is a visible journey: it began by bringing separate hardware lines under one dashboard, with the Meraki dashboard extending to manage Catalyst hardware, and it continues into Cisco Cloud Control, a cross-domain plane built open to third parties by design. Cisco's particular advantage is breadth. Where many platforms stop at networking and security, Cloud Control spans the Cisco portfolio across networking, security, collaboration, data center, compute, observability, and the Splunk-based data layer, removing more of the fragmentation tax precisely because it reaches more domains. It is also open: Cloud Control integrates dozens of third-party platforms through native connectors and MCP, already including competitive solutions such as the identity providers Okta and Microsoft Entra ID, and its Agent Builder and App Builder let customers and partners connect almost any API-driven, agentic system, building their own connectors where no native one exists. Independent analysts have recognized the direction: Cisco was named a Leader in the 2026 Gartner Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, on an architecture built around operational simplicity, security built into the network fabric, and AI-ready infrastructure. Two honest caveats: Cisco Cloud Control is in Controlled Availability today, and the Studio builders with customer-built MCP connectors are targeted for late 2026.

3. The Blueprint

Sequence is the principle. Start where your refresh cycle or your existing footprint puts you, and add capability in an order where each step earns the next.

Three properties make this a blueprint, not a wish list:

- **Each phase stands alone.** Stop after Phase 1 and you still gained one plane and faster deployment.
- **Each phase has exit criteria.** You know when the next phase is earned.
- **Nothing is thrown away.** Plane, automation, and telemetry investments compound rather than reset.

It is also a growth path. The same plane that delivers simplicity at 300 people carries the organization into mid-market and enterprise operations as it grows.

The spine: Consolidate → Automate → Activate → Orchestrate.

4. Phase 1 — Consolidate

Promise: one plane to deploy and run the network, no matter which domain you start with.

Business outcome: sites stand up in hours instead of weeks, and one team runs them all.

Entry into this phase usually tracks the hardware refresh cycle. A team rarely refreshes wireless, switching, and routing at the same time, so the practical entry point is whichever domain is up for renewal first. This is deliberate: the blueprint does not ask for an entire forklift. Some vendors have backwards compatibility for older hardware to be onboarded into a modern management platform. No refresh is required to begin. Consolidation is also not a one-time step. As the later phases proceed, additional domains keep moving onto the same plane, the cloud-managed dashboard and, as the estate broadens, the unified cross-domain console, so this phase effectively runs throughout the journey.

The win in this phase is not just a single console. It is the elimination of the per-site, per-device manual work that consumes a lean team. Zero-touch onboarding and templated, low-code automation let a small team bring up a new site or a new device without scripting expertise or a truck roll, which is the first and most tangible repayment of the fragmentation tax.

What to look for (any vendor)

- A **cloud-managed networking platform** that unifies at least wired, wireless, and WAN under one console with templated, zero-touch provisioning.
- **Low- or no-code automation** that orchestrates device onboarding and branch bring-up, ideally across both your own and third-party systems, so site turn-up does not depend on a scripting specialist.
- **Included, not bolted on.** The automation and management layer should come with the platform, not as a separate purchase that adds to the tax.

The Cisco recommendation. The network is operated from the **Meraki dashboard** supporting new unified hardware as well as legacy Meraki and Catalyst products in wireless, wired and WAN. For deployment, **Cisco Workflows** is embedded in the Meraki dashboard as a low-/no-code automation application: it ships with validated templates for automated branch bring-up that run inventory pre-checks, onboard devices, and establish connectivity, and it can orchestrate across both Cisco and third-party systems. It is included at no additional cost with an active Cisco network management license, which makes it part of the compounding-value story from day one rather than another tool to buy. On top of the dashboard, the **Cisco Cloud Control** entitlement is also included at no additional cost with an eligible subscription; it is in Controlled Availability today, so meaningful day-to-day use typically begins in later phases, but the entitlement starts here.

What you deploy

- One **Meraki-managed Cisco component** (access point, switch, or router) with a **Essentials or Advantage** subscription. Lead with whatever is supported today or up for refresh.
- For organizations with existing Catalyst hardware, note that most of the Catalyst 9000 access points, wireless controllers and switches can be onboarded to the Meraki dashboard. Through Cisco Cloud Entitlement for DNA, you can use your existing DNA licenses to enable cloud-managed capabilities with no additional purchase needed.

Included at no additional cost

- **Cisco Workflows** low-/no-code automation, within the Meraki dashboard.
- **Cisco Cloud Control** entitlement (Controlled Availability).

Exit criteria. Phase 1 is complete when at least one access domain is cloud-managed from a single console with templated configuration that new sites inherit, and new device or site bring-up no longer requires manual, per-device configuration.

5. Phase 2 — Automate

Promise: AI runs the day-to-day, so the team resolves issues faster and stops doing repetitive work.

Business outcome: lower mean-time-to-resolution, fewer tickets, and less-experienced staff operating effectively above their level.

With the estate on one plane, the next repayment of the fragmentation tax is operational. Routine triage, tuning, and troubleshooting move from people to AI. A natural-language assistant answers "why is this site slow" in seconds instead of a multi-console investigation, and advanced analytics and policy automate the work that used to require a senior engineer.

What to look for (any vendor)

- An **AI assistant for operations** that supports natural-language troubleshooting against the plane's own telemetry.
- **Automated tuning** (for example, RF and QoS optimization) and **anomaly detection** that reduce alert load rather than add to it.
- **Advanced policy and analytics** available as an in-place capability tier, so adopting them is activation, not a new integration.

The Cisco recommendation. The **Meraki AI Assistant** provides natural-language troubleshooting, and the **Advantage** license tier unlocks the advanced capabilities (Adaptive Policy, AI-driven radio resource management, advanced security). A note on value: if you already chose Advantage in Phase 1, **Phase 2 is not a new purchase. It is value you have already paid for, waiting to be switched on.** The work is activation: turning licensed capability into realized outcomes, fewer tickets, faster resolution, and more of your team's time returned to the business. If you landed on Essentials, Phase 2 is the natural step up to Advantage when those outcomes justify it.

What you deploy

- **Meraki Advantage** tier, only if it was not already purchased in Phase 1.

Already owned / activate only

- **Cisco AI Assistant for Networking** and the **Advantage** feature set, if you are already at that tier.
- **Proactive Packet Capture**

Exit criteria. Phase 2 is complete when AI-assisted troubleshooting is in regular use and advanced analytics or policy capabilities are active on at least one product class.

6. Phase 3 — Activate: Security & Assurance

Promise: a resilient network, secured and assured from the plane you already run.

Business outcome: zero-trust access, microsegmentation, and deep-path assurance at lean-team operating cost, with no appliance sprawl.

In this phase the access estate becomes the platform for the capabilities a network team increasingly owns alongside connectivity: security and assurance. These are adjacent disciplines, and activating them from the same dashboard, rather than as standalone appliances and consoles, is the clearest demonstration that consolidation compounds value instead of adding tax. Three pillars define a resilient network: **zero-trust access**, **microsegmentation**, and **deep-path assurance**. Together they answer the questions a lean team cannot otherwise resolve: who and what is allowed to connect, whether a compromised device can move laterally, and whether a slowdown is yours or the provider's.

What to look for (any vendor)

- **Zero-trust network access** that ties access to verified identity and device posture rather than network location, replacing implicit-trust remote access.
- **Cloud-delivered NAC and identity-based microsegmentation** that does not require a fleet of dedicated appliances.
- **Deep-path, end-to-end assurance** that distinguishes your network from the ISP from the SaaS provider.
- **Cross-domain threat detection and response (XDR)** that correlates signals across endpoint, network, and cloud, for teams ready to fold security operations into the same plane.
- **Single-plane operation**, so each new capability is managed where the team already works, not in a new console.
- **A path for mixed estates**, so multi-vendor environments are not excluded from access control or assurance.

The Cisco recommendation:

- **Zero Trust Access - Secure Access:** Natively integrates through Meraki AutoVPN to deliver a unified Secure Access Service Edge (SASE), enforcing least-privilege, direct-to-cloud application access that protects users and data everywhere without backhauling traffic or compromising network performance.
- **Zero Trust Identity and Posture - Duo:** Serves as the continuous verification engine across the Meraki fabric by enforcing adaptive multi-factor authentication and strict device health checks, guaranteeing that only verified users on compliant devices can connect and feeding vital identity context directly into Meraki's Adaptive Policy segmentation.

- **Proactive Experience Monitoring** ensures end-to-end visibility by combining ThousandEyes for external WAN and SaaS tracking with Meraki Insight for internal network health.

What you deploy

- **Cisco Access Manager, Secure Access and Duo** license

Already owned / activate only

- **ThousandEyes** and **Meraki Insights** entitlement through Advantage license tier

Exit criteria. Phase 3 is complete when zero-trust access and identity-based microsegmentation are enforced and deep-path assurance (user to ISP to SaaS) is active, all operated from the existing plane.

7. Phase 4 — Orchestrate

Promise: run the whole estate as one agentic system, with people in the loop where it counts. *Business outcome: cross-domain investigation in plain language, context that survives shift handoffs, and a team that scales with the business instead of with headcount.*

(This phase can run in parallel with Phases 2 and 3, depending on your existing assets, expansion plans, and availability of a single operating platform.)

This is where compounding value and the fragmentation tax meet head-on. As other domains enter the estate (security, collaboration, data center, compute, observability, and data fabric), a cross-domain operating layer either unifies them or the tax returns at enterprise scale. The end state is one operating model where AI agents handle routine monitoring and investigation across domains, and people approve consequential change.

What to look for (any vendor)

- A **cross-domain operations layer** that correlates networking, security, and other domains in one view.
- **AI-assisted, natural-language investigation** that works across domains, not within a single tool.
- **Agentic automation with human-in-the-loop governance**, so routine work is delegated safely and consequential change is approved by a person.
- **Included with what you already own**, so unification does not become its own new cost center.

The Cisco recommendation. **Cisco Cloud Control** is the cross-domain plane, with **AI Canvas** as the shared workspace for human-and-agent investigation. As Cisco domains enter the estate, Cloud Control unifies them under one login and one view at no new license or cost for eligible subscriptions, which is the structural antidote to the fragmentation tax: the more you consolidate onto it, the more it is worth. **Cloud Control Studio** (Agent Builder and App Builder)

extends this to custom and ambient agents, with capabilities maturing through 2026. On sequencing: this phase is not strictly after Phase 3. If you are already invested in Cisco security or collaboration, you can begin cross-domain unification in parallel, gated mainly by Cloud Control's progression from Controlled to General Availability.

What you deploy

- **Nothing new for Cloud Control itself** on eligible subscriptions. Value scales with each additional Cisco domain attached.

Optional / roadmap

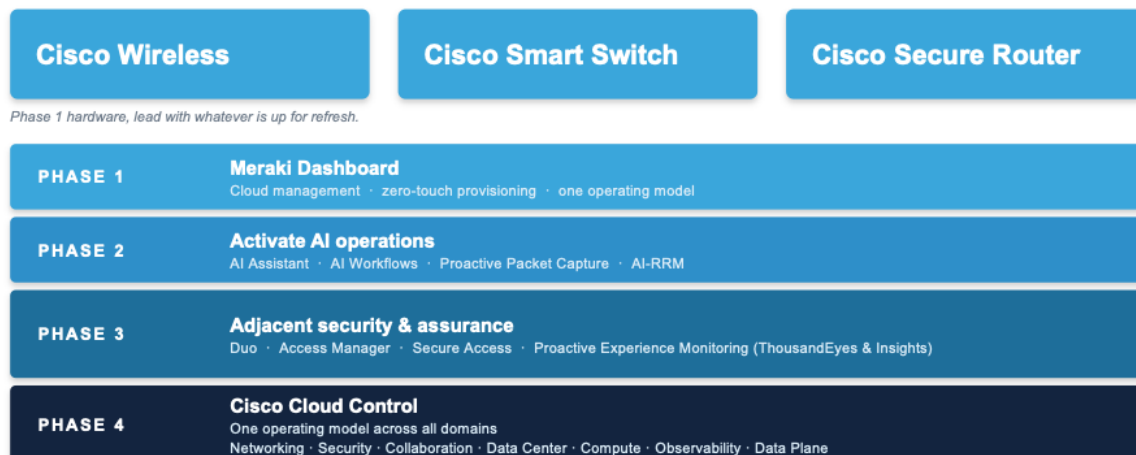
- **Cloud Control Studio** (Agent Builder, App Builder) for custom and ambient agents, maturing through 2026.

Exit criteria. Phase 4 is complete when a multi-domain estate is operated from one plane with agent-assisted workflows and human-in-the-loop governance.

One Plane, Built Phase by Phase

Start with the hardware. Each phase adds a layer, all managed from one plane.

WHAT YOU DEPLOY



Cisco Confidential

8. Where to Start

The blueprint meets you where you are, on whatever infrastructure you run today.

Refreshing hardware soon? Start Phase 1 with the domain that is up for renewal. One Cisco-branded, Meraki-managed component puts you on the plane without a forklift.

Already on the Meraki dashboard? You are already in Phase 1. Move directly to Phase 2 by activating the AI assistant and the Advantage features, then to Phase 3.

Already paying for an identity provider or productivity suite? Keep it. Phase 3 access control integrates with the identity you have; the blueprint adds the network-side capabilities a productivity suite does not include.

Running a mixed or competitor estate? Use the brownfield paths: ThousandEyes for vendor-neutral assurance and Cisco Workflows to orchestrate across third-party systems. For access control, ISE suits Cisco-leaning estates, while a genuinely multi-vendor estate may be better served by a vendor-agnostic NAC. Consolidate over time rather than all at once.

Running lean? The blueprint assumes it. Lead with one plane and automation so a small team is not buried in consoles, and use a partner or managed service for delivery. Every phase boundary doubles as a natural quarterly review.

The Cisco recommendation. If you would rather not assemble this from parts, Cisco delivers all four phases as one operating model, the Meraki dashboard today and Cisco Cloud Control as it reaches General Availability, available directly or through Cisco partners as a managed service. The advantage is the fewest consoles, the fewest integrations, and an estate where every addition compounds value instead of tax.

9. Getting Started

A short assessment is the low-friction first step. A **Phase 1 readiness review**, run against your refresh schedule and current footprint, should return three things: a map of which domains are on a single plane today and which are not, an estimate of the manual deployment and troubleshooting effort the current model costs (the fragmentation tax you are paying now), and a recommended entry phase with exit criteria.

From there, the sequence is one this paper already wrote. Contact your Cisco account team or partner to run the readiness review.

Appendix A — Capability-to-Cisco Mapping

Phase	Capability you need (any vendor)	Cisco recommendation
1 — Consolidate	Cloud-managed networking + zero-touch, low-code deployment automation	Meraki dashboard · Cisco Wireless / C9350 Smart Switch / 8000 Series Secure Router · Cisco Workflows (included) · Cloud Control entitlement (CA, included)
2 — Automate	AI ops assistant + automated tuning + advanced policy tier	Meraki AI Assistant · Advantage tier (activate or tier-up)
3 — Activate	Zero-trust access + microsegmentation/NAC + deep-path assurance (+ XDR)	Cisco Secure Access · Cisco Access Manager (or on-prem ISE for mixed estates) · ThousandEyes · Cisco XDR (suggested) · MG · MV

Phase	Capability you need (any vendor)	Cisco recommendation
4 — Orchestrate	Cross-domain ops layer + agentic, human-in-the-loop automation	Cisco Cloud Control · AI Canvas · Cloud Control Studio (roadmap)

Appendix B — Phase Exit-Criteria Checklist (printable)

- **Phase 1 complete when:** at least one access domain is cloud-managed from one console with templated config / new site and device bring-up requires no manual per-device configuration.
- **Phase 2 complete when:** AI-assisted troubleshooting is in regular use / advanced analytics or policy active on at least one product class.
- **Phase 3 complete when:** zero-trust access and identity-based microsegmentation enforced / deep-path assurance (user to ISP to SaaS) active / all operated from the existing plane.
- **Phase 4 complete when:** multi-domain estate operated from one plane / agent-assisted workflows with human-in-the-loop governance.

Appendix C — Status Legend and Sources

Status legend. GA: Generally Available. CA: Controlled Availability. Beta / Roadmap: as labeled.

Current statuses referenced: Cisco Cloud Control is in Controlled Availability (US, June 2026, global to follow). Cisco Access Manager is GA (November 2025). ThousandEyes on the Meraki MX is GA; ThousandEyes embedded on cloud-managed switches is in Beta. Cisco Workflows is GA and included with an active Cisco network management license. Cloud Control Studio, Agent Builder, and App Builder are roadmap items targeted through 2026.

Sources. Gartner, 2026 CIO Agenda and 2026 CIO and Technology Executive Survey (cost optimization and productivity as top business outcomes; ~52% of CIOs citing cost reduction as a growing priority); Gartner, "CIOs: Focus cost optimization on funding growth, not cutting costs." Freshworks, The Global Cost of Complexity Report: The Mid-Market AI Complexity Trap (May 2026), survey of 12,021 IT professionals including more than 9,000 in mid-market organizations. EMA observability research and Cisco Splunk internal data on tool sprawl and the "toggle tax" (attribution to be confirmed against the primary EMA report before publication). Industry usage of the "fragmentation tax" concept across operations and IT. Cisco product documentation: Cisco Workflows (Cisco Networking Cloud); Cisco Access Manager; Cisco Secure Access; Cisco ThousandEyes (Meraki integration); Cisco XDR; Cisco Cloud Control and AI Canvas; Cisco ISE network component compatibility. Full citations to be compiled in the technical companion before publication.