Cisco Executive Brief

JULY 2026

A New Operating Model for Critical Infrastructure

Executive brief on cyber defense in the AI era

Table of Contents

The shift to continuous defense

Frontier AI models have fundamentally altered the threat landscape. These systems now identify vulnerabilities, write exploits, and chain them into attack paths at machine speed. This isn't a temporary cycle you patch through. It's a permanent shift in how fast your environment can be compromised.

Two forces rewriting risk

01 The patch cycle has been outpaced

The time from disclosure to active attack was already collapsing. Frontier AI compressed the timeline to hours.

02 The barrier to entry has vanished

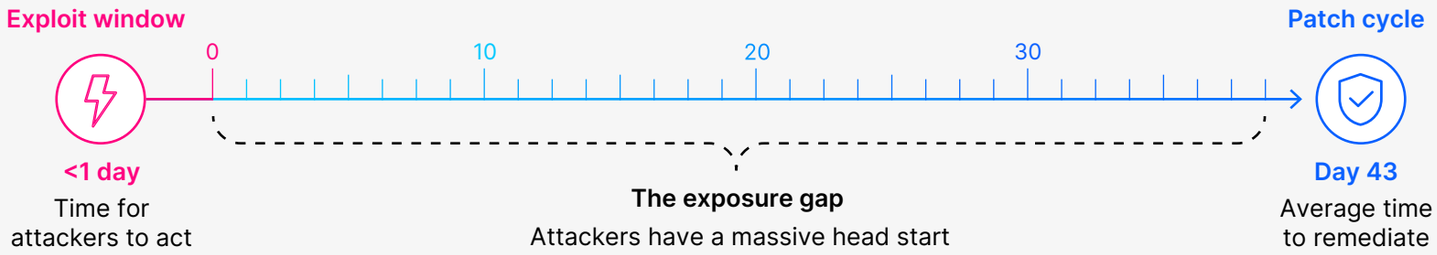
AI gives low-skill attackers the ability to execute sophisticated techniques that once required nation-state resources.

These forces compound: faster exploitation widens the set of weaknesses an attacker can reach, while a lower barrier to entry widens the set of attackers who can reach them. More opportunities, in more hands, at higher speed.

Organizations struggle to defend this new reality for two reasons: aging infrastructure that can't be patched or upgraded for protection and outdated processes that treat infrastructure security as a periodic, manual event.

The legacy model that's persisted—harden, validate, and maintain—assumes adversaries operate within the constraints of your maintenance calendar. They don't.

The data exposes the risk of this approach: in 2025, 40% of the most targeted vulnerabilities hit end-of-life systems. The median time to patch a critical vulnerability remains 43 days. But the exploit window, which is the time between disclosure and weaponization, is now hours. Against that reality, 43 days is not a delay. It's the whole game.



40%

TARGETED VULNERABILITIES HIT EOL SYSTEMS

They can't be patched. They stay exposed.

Why the gap is so dangerous:

Sources: *Talos Year in Review* and *2026 Verizon Data Breach Investigations Report*

A new operating rhythm

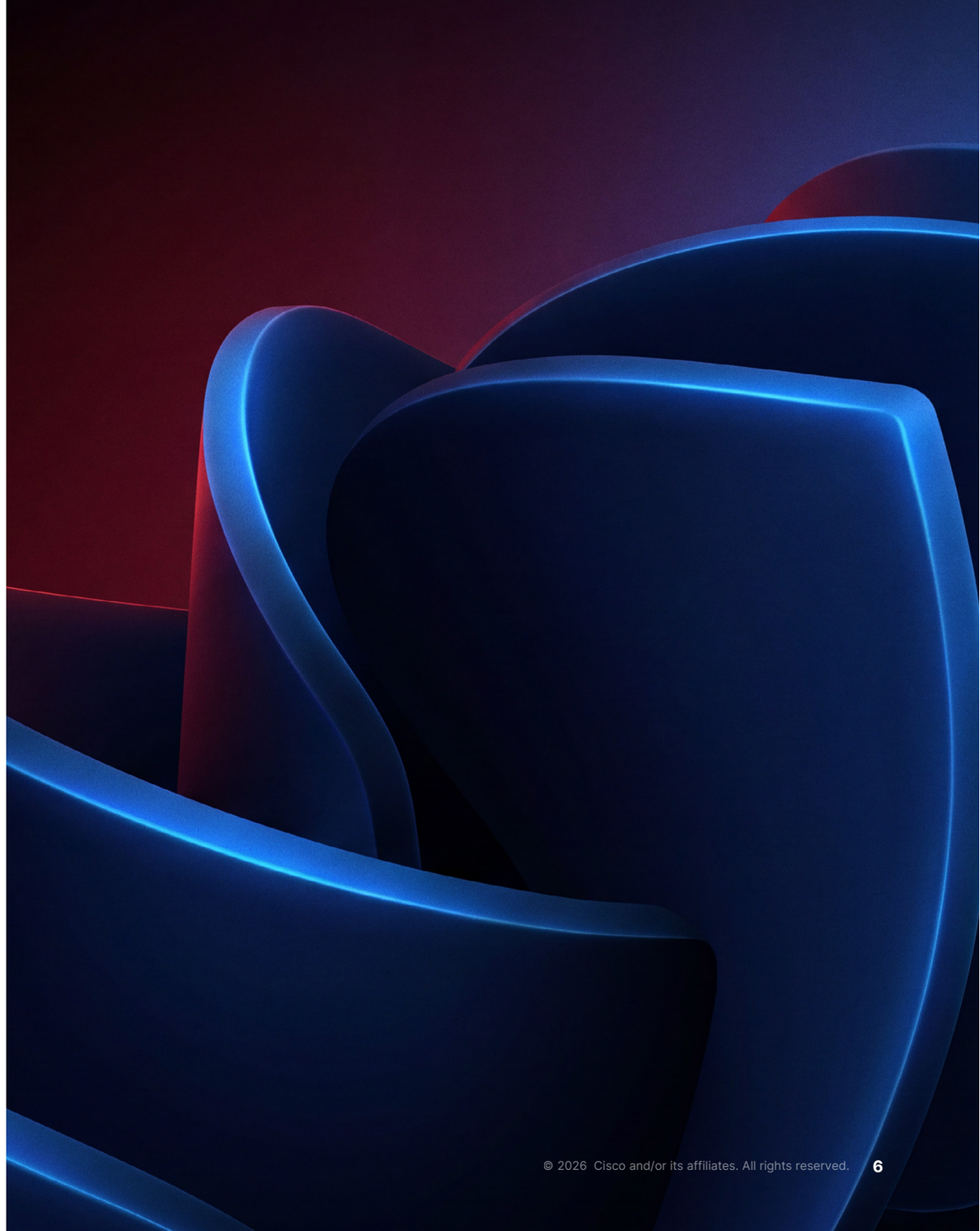
You can’t outpace AI-era threats using legacy processes or legacy technology. What’s needed is a continuous operating rhythm: align patches and upgrades to a frequent, predictable cadence, retire assets that can’t be secured, and aggressively reduce exposure year-round.

This executive brief outlines the practical steps to protect your organization in the AI era: advance your operating model, modernize your infrastructure, and elevate your security posture. Review these steps jointly with your security and networking leads—approaching in a single domain leaves the door open to unnecessary risk.

When you’re ready to move, your Cisco account team can share a detailed playbook to provide your network and security teams with deeper, practitioner-level guidance on the information shared in this brief.

From theory to practice: Defending at machine scale

Frontier AI is changing offense and defense, but not equally. As Rich Mogull, Chief Analyst at Cloud Security Alliance, describes in a recent report, attackers have a mathematical advantage: they only need to find one vulnerability to exploit. Defenders must secure every resource, from every attacker, every time. You can't beat this math with legacy processes. To take back the advantage, you need an operating model that helps harden code, patch faster, and defend continuously at scale.



Cisco is already putting this model to work

> “In just eight weeks, we scanned 1.8 billion lines of code across the breadth of Cisco’s portfolio, a process that would have taken our security research team eight years. We are only getting started.”
>
> **Anthony Grieco**
> Senior Vice President and
> Chief Security & Trust Officer
> Cisco

Defenders need more than access to powerful AI models. They need the expertise and operating model to turn AI’s speed and scale into repeatable security outcomes. The Cisco Security and Trust organization proved the approach inside our own environment first, pairing frontier AI with security expertise and dedicated resources to find and fix vulnerabilities faster, make evaluation repeatable, and move prevention upstream.

- **Find and fix faster:** Through early participation in Anthropic’s Project Glasswing and OpenAI’s Trusted Access for Cyber (TAC), Cisco applied frontier AI models across its own portfolio, analyzing 1.8 billion lines of code across 25+ languages in eight weeks. The work showed how defenders can use AI speed and scale to accelerate vulnerability discovery and remediation across real enterprise code.
- **Make evaluation repeatable:** Informed by that internal security engineering work, Cisco open-sourced the Foundry Security Spec, a battle-tested blueprint for building agentic security evaluation systems. The spec gives defenders a model-agnostic, stack-agnostic way to move from noisy alerts to bounded, prioritized, verifiable findings.
- **Move prevention upstream:** Cisco built and open-sourced Project CodeGuard to bring secure-by-default rules into AI coding workflows. When paired with Foundry Security Spec, confirmed gaps can become reusable rules, helping prevent known bug classes before they reach production.

Defining the new operating model for critical infrastructure

We believe organizations need to shift to a continuous defense across three dimensions: cadence, modernization, and posture.

This continuous model changes how you operate: patching becomes an ongoing rhythm instead of a fire drill, modernization retires risk instead of just refreshing hardware, and a dynamic security posture shrinks the blast radius of any breach.

	The old approach Harden it, prove it, don't touch it	**The post-Mythos approach** Harden it, prove it, continuously defend it at machine speed
Cadence	Major upgrades every 12–24 months	Continuous, CI/CD-style release readiness
Modernization	Aging gear, protocols, and scripts kept in service	Continuous removal of what can't be made safe
Security posture	Documented risk exceptions	Continuous exposure reduction and containment

Start here: Three priorities

Change begins with three priorities: running resilient infrastructure to support your business, addressing aging infrastructure, and elevating your overall security posture. Here's a summary of these priority areas and the questions you can ask your team to get started.

1. Advance your operating model for resilient infrastructure

Patching isn't a periodic project anymore; it's a continuous capability. The math forces the shift: fix volume is rising while maintenance windows shrink, and manual, device-by-device processes can't close that gap—adversaries can exploit that lag. The answer is a predictable, automated cadence, where automation absorbs the volume, so your engineers spend their time on judgment calls, not device-by-device execution. Then make the cadence enforceable: set remediation SLAs by exposure tier, closing internet-facing exposures within days and the next tier in the next window.

ASK YOUR TEAM:

- What is our current median time from advisory to verified closure by exposure tier?
- Which steps are still manual?

2. Modernize your infrastructure

Unsupported assets carry a risk no control can offset: when the next vulnerability lands, there is no patch coming. You can't remediate what the vendor no longer maintains, you can only contain it or retire it. That's why modernization isn't a refresh conversation; it's a risk-retirement conversation, and the business case runs on exposure and lifecycle data, not equipment age. Standardize on one architecture you can patch, see, segment, and prove—then fund it as a security requirement, sequenced in waves against your highest-exposure assets first.

ASK YOUR TEAM:

- How many assets are past or nearing last day of support?
- What do they connect to, and what's the cost to keep them another year?

3. Elevate your security posture

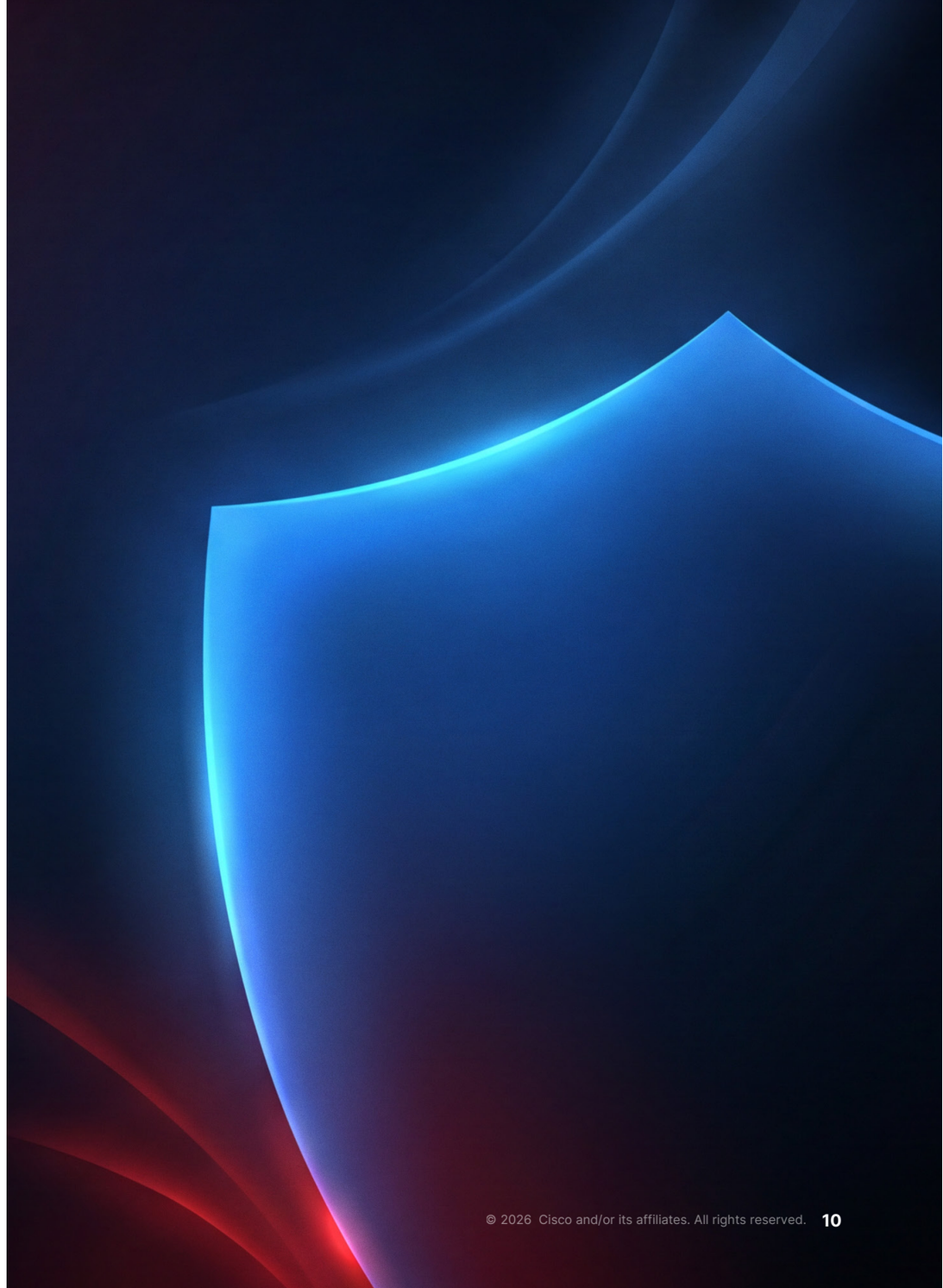
AI-driven adversaries can now chain vulnerabilities at machine speed, putting your infrastructure at risk. Shield exposed assets to reduce your attack surface. Segment your environment to contain breaches and limit their blast radius. Close hidden identity gaps to prevent escalation. As attack speeds outpace human teams, your SOC needs the visibility, automation, and agentic AI workflows to keep pace.

These controls aren't all new, but their urgency is. Putting them in place now is what keeps you ahead of the attacker of the near future, not just the rare advanced one today.

ASK YOUR TEAM:

- If an attacker got a foothold today, how far could they move across the attack path before we contained them?
- How would we know?
- How fast could we respond?

Once you set these three priorities, the focus shifts from technical strategy to business execution and measuring success.



Measuring success and securing the budget

Measure what matters and frame the investment around business risk to secure the budget.

Measuring success

- **Track advisory-to-closure time.** Measure by exposure tier.
- **Measure estate currency.** Track the percentage of your environment running the latest release.
- **Enforce remediation SLAs.** Focus on tier-based service level agreements rather than raw vulnerability counts.
- **Maintain board-ready evidence.** Keep compliance records, remediation timelines, and asset status ready for auditors and cyber-insurers.
- **Mandate accountability for agentic work.** Ensure every consequential action is auditable and reversible, with a named human owner.

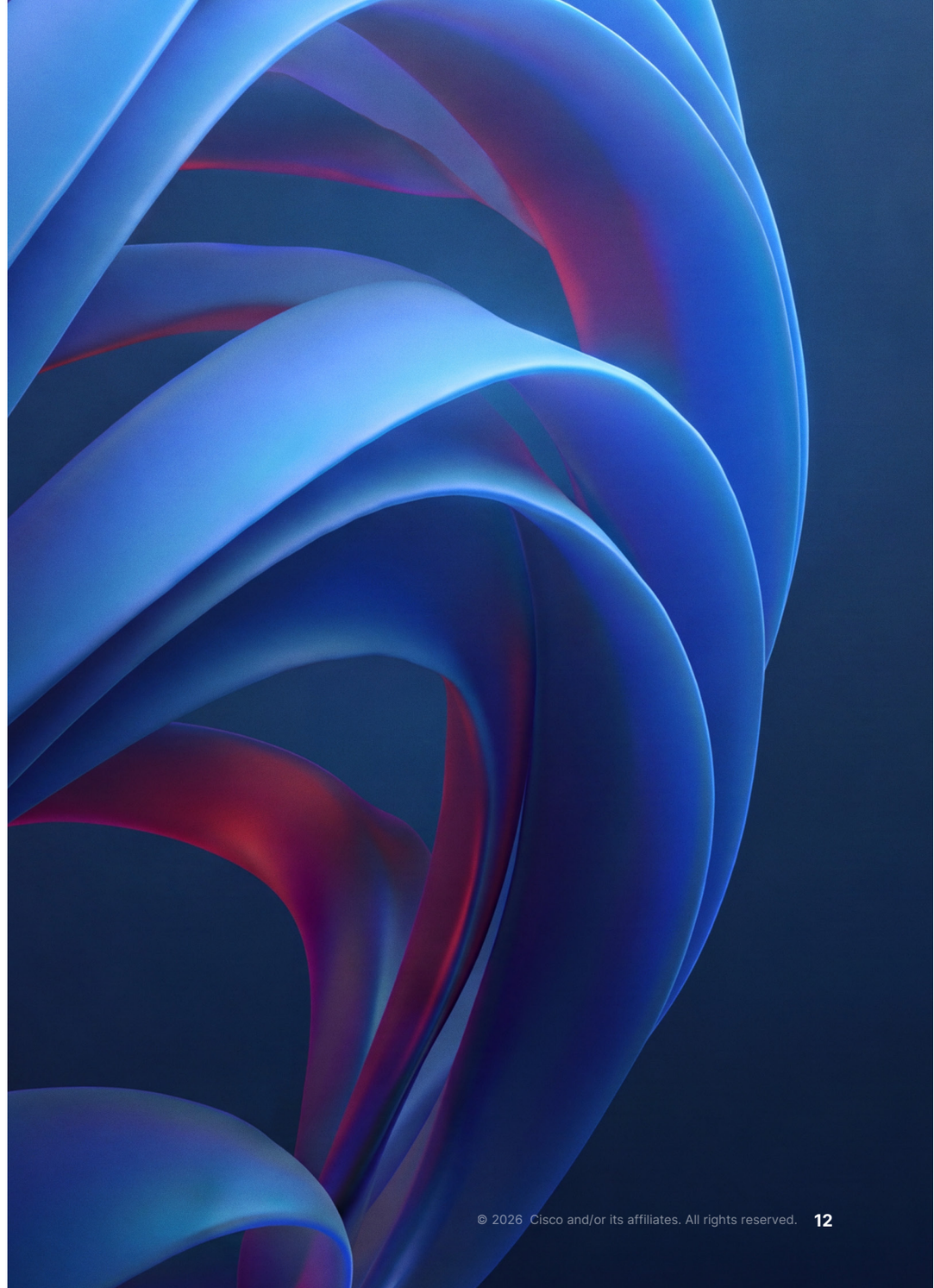
Funding the new model

- **Sequence the spend.** Tie each modernization wave to a budget cycle, targeting the highest-exposure assets first.
- **Align spend with timing.** Use financing to convert unplanned capital into predictable payments.
- **Frame as a security requirement.** The threat sets the deadline. This is a business imperative, not a wish-list item.
- **Fund operational capacity.** Budget for services and partners to scale your team's efforts without adding headcount.

The first 90 days

Here are five action items you can authorize now. None require the full program to be designed first, and each one makes the next easier.

1. **Start an exposure assessment.** Establish one current, prioritized view that shows what you have, what's vulnerable, what's unsupported, and what's at risk. This will serve as your shared source of truth.
2. **Set remediation SLAs by exposure tier.** Commit to closing internet-facing or high-criticality exposures within days and the next tier in the next window, and report against it. This is the policy decision that makes continuous defense real.
3. **Stand up the cadence.** Standardize change windows and pre-approve templates so that patching becomes routine maintenance rather than an exception.
4. **Name the first wave of modernization targets.** Identify the highest-exposure unsupported assets and fund their replacement first, with the business case built on exposure, lifecycle data, and future business needs. Modernization is an opportunity to bring in more secure, future-ready infrastructure.
5. **Run an AI-era response tabletop exercise.** Simulate an adversary exploiting an edge vulnerability to move laterally at machine speed, aligning teams on response.



How Cisco helps

Cisco and our trusted partners are here to help you navigate this new reality. Along with our partners, we offer professional services to help your organization across all these areas, including Cisco Resilient Infrastructure Services, which provides a three-phased structured approach to infrastructure hardening.

Advance your operating model for resilient infrastructure:

Starting in July 2026, Cisco releases on a fixed schedule with advance notice, staggered so no team faces two major windows at once. We map each advisory to your assets, rank it by exposure, not severity score alone, and confirm the fix landed. When a patch or upgrade can't be deployed yet, runtime shields protect the asset with no downtime.

Modernize your infrastructure:

We offer several ways to help you see what Cisco assets are unsupported and exposed, plus recommendations for hardening infrastructure and enabling additional security protections. When considering a refresh with modern infrastructure, Cisco recommends a secure networking architecture that fuses security into the network itself—with identity-first segmentation, common policy, and distributed enforcement. To help along the way, Cisco Capital offers financing options to manage unplanned expenditures.

Elevate your security posture:

Cisco secures the full attack path: identity governed across human, machine, and AI-agent entities—a distinction that matters more as agents multiply; segmentation enforced to contain lateral movement when a breach happens; and detection and response accelerated to machine speed, with AI absorbing the volume and your analysts keeping the judgment calls.

Continuing the conversation

When you're ready to move, contact your Cisco account team to help you turn this brief into action. They can guide you on this journey, walking you through a more detailed plan and assessment bespoke for your organization and its challenges.

Your Cisco Partners are also a great resource. Partner capabilities vary, so match a partner's strengths to your environment. Visit the Cisco partner hub to find the right fit.