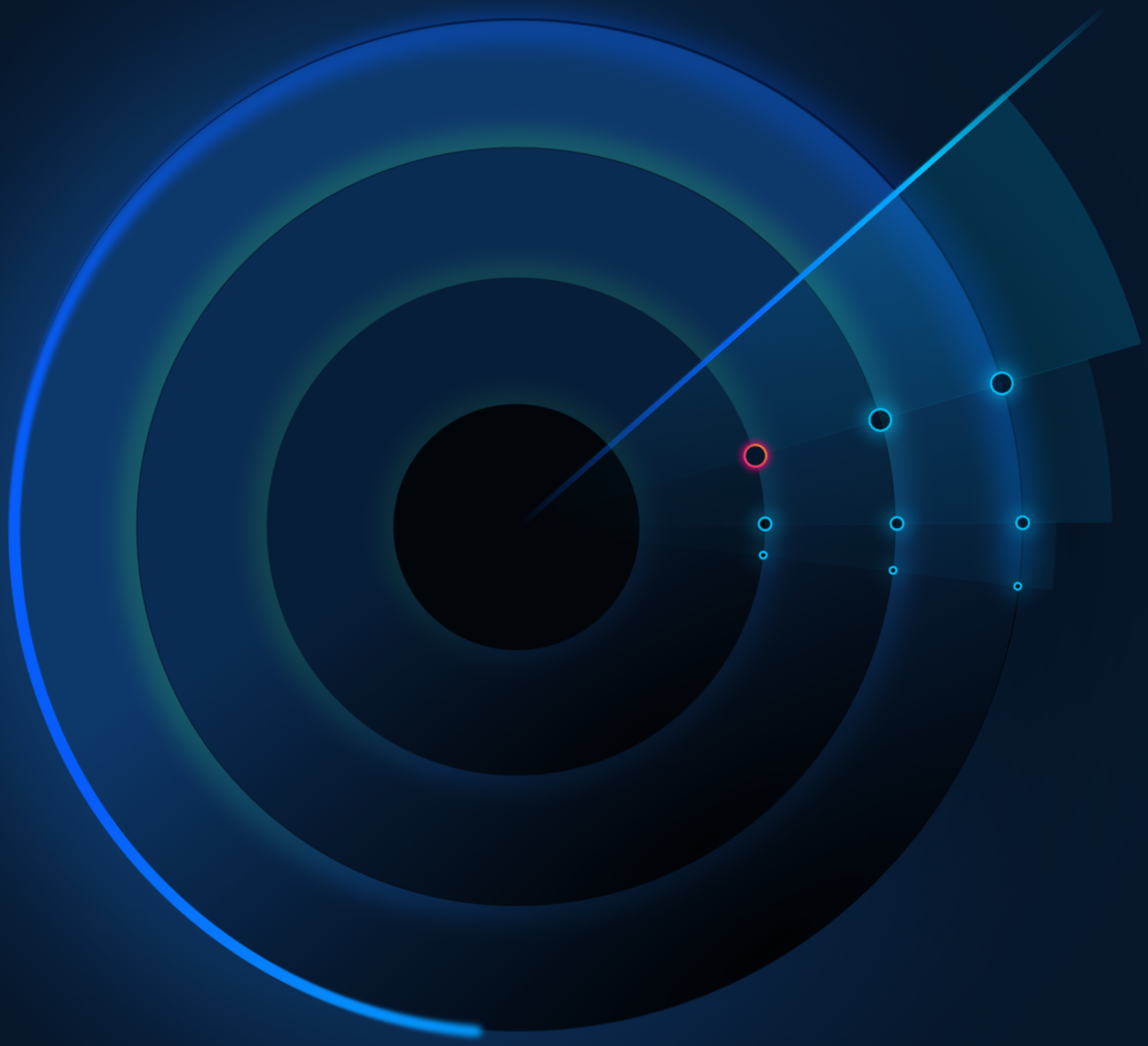
Building Infrastructure Resilience for Defense in the AI Era

The fundamentals of infrastructure resilience haven't changed, but the pace and scale have. Cisco® Resilient Infrastructure Services leverage Cisco IQ, where human expertise meets agentic intelligence, to help organizations respond to AI-accelerated threats and vulnerabilities faster.



Contents

INTRODUCTION

The Rules of Engagement Have Changed

Organizations have always faced infrastructure risk. What's changed is the pace and scale.

Advances in AI are fundamentally changing how vulnerabilities are discovered, analyzed, and exploited. In 2021, adversaries took a year to reach exploit from the time a vulnerability was disclosed; in 2026, that window has collapsed to a mere few hours[1]. Using frontier models, attackers are rapidly identifying not only new weaknesses but also vulnerabilities that have existed for decades. They can chain together multiple vulnerabilities into viable attack paths and operate at a scale and speed that traditional defensive processes were never designed to match.

The result is a daunting new reality for infrastructure security and IT teams. The challenge is no longer just finding vulnerabilities or applying patches. Organizations struggle with a lack of visibility—organizations rely on manual, slow mapping processes that cannot keep pace with the speed and scale of today's AI-driven threats needed to identify which exposures pose the greatest business risk. Teams also face complex structural hurdles, including aging infrastructure that has reached EoL (end-of-life), LDOS (last-day-of-support), or EoVSS (end of vulnerability/security support), and the need for better threat containment by implementing micro-segmentation and Zero Trust—never trust, always verify—principles. Because software upgrades are only a subset of the necessary actions, teams must move beyond manual triage to rapidly assess, prioritize, and remediate these complex gaps before attackers can exploit them.

For many organizations, the information needed to make those decisions remains disconnected, and teams are left manually correlating data across multiple systems while the window to respond continues to shrink.

1. Source: Zero Day Clock, "The Collapse"

When Time Becomes the Critical Resource to Achieve Resilience

As AI compresses the time between vulnerability discovery and exploitation, the obsolescence of existing operational models is laid bare. Organizations need to create an operating model that continuously connects visibility, prioritization, and action before attackers can exploit the gap.

That begins with visibility. Today's infrastructure—spanning campus, branch, and edge environments—is often trapped in operational silos. When inventory and asset data are fragmented across these sites, you lose the unified visibility required to defend your network. This lack of centralized intelligence creates critical blind spots, leaving your environment exposed to risks that move faster than your ability to detect and remediate them. Visibility alone, however, doesn't create resilience.

Not all vulnerabilities carry the same risk, and not all assets are equally critical to your business. You need to correlate asset inventories, lifecycle health (such as support status and EoL milestones), software versions, and security posture to distinguish urgent issues from the background noise. Prioritizing these critical gaps allows your team to focus on finite resources where they have the greatest impact.

At the same time, resilience depends on the infrastructure itself. Systems that are beyond their EoL and LDOS accumulate technical debt, slowing remediation efforts and limiting an organization's ability to respond as threats evolve. Modernizing infrastructure isn't simply an upgrade. It's a way to make sure aging assets aren't discovered only after an incident that puts the organization at risk.

Building resilience also requires a continuous operating model that brings these capabilities together. With ongoing visibility into the environment, continuous lifecycle management, exposure mapping, and security monitoring, organizations can prioritize modernization efforts and respond more quickly to evolving threats.

Introducing Cisco Resilient Infrastructure Services

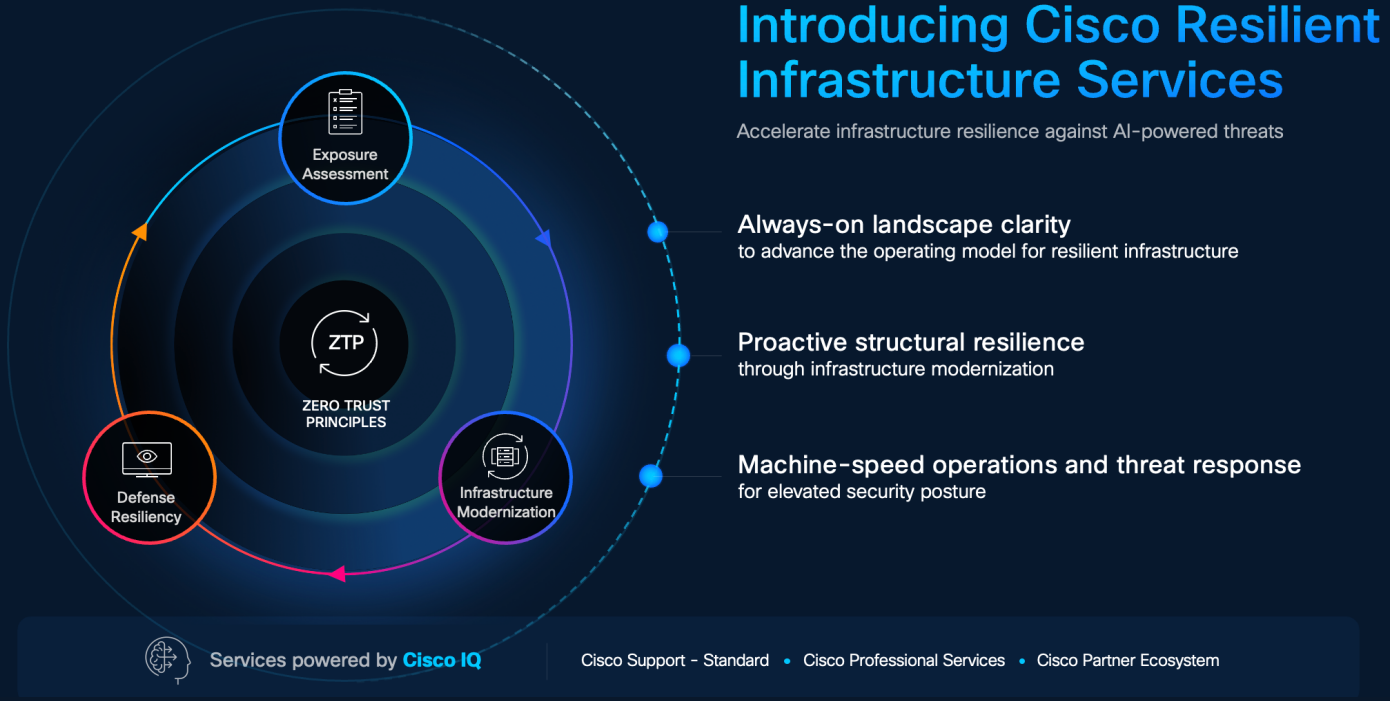
Cisco Resilient Infrastructure Services simplify, accelerate, and de-risk your infrastructure resilience journey. By combining the collective capabilities of Cisco Support and Professional Services, including Cisco IQ's agentic intelligence, it can replace fragmented, manual processes with a machine-speed operating model.

Our approach is built on three strategic pillars:

1. **Exposure Assessment:** Immediate discovery and prioritized risk mapping for always-on landscape clarity, digitizing the process with a Resilient Infrastructure playbook within Cisco IQ.
2. **Infrastructure Modernization:** Proactive structural resilience and operational agility, combining AI, automation, and specialized experts to de-risk and accelerate infrastructure modernization.
3. **Defense Resiliency:** Expert-led, continuous, autonomous protection with AI-driven enforcement for machine-speed operations and threat response.

This unified strategy can save your team from drowning in endless patching cycles, where you are reacting to every alert without knowing if your most critical assets are truly protected, to a proactive stance that swiftly outpaces frontier model threats.

This critical journey begins with **Cisco Support–Standard**, which integrates Cisco IQ AI-powered capabilities to transform data-driven insights into prioritized, guided actions that power the Cisco Resilient Infrastructure Services playbook.



A Guided Path to Infrastructure Resilience

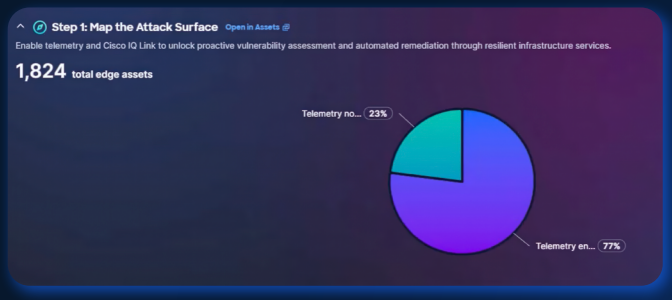
Cisco IQ serves as a defender's roadmap—delivering the clarity teams need to fully understand their environment, prioritize critical risks, and take action with greater speed and confidence.

Attack Surface Mapping

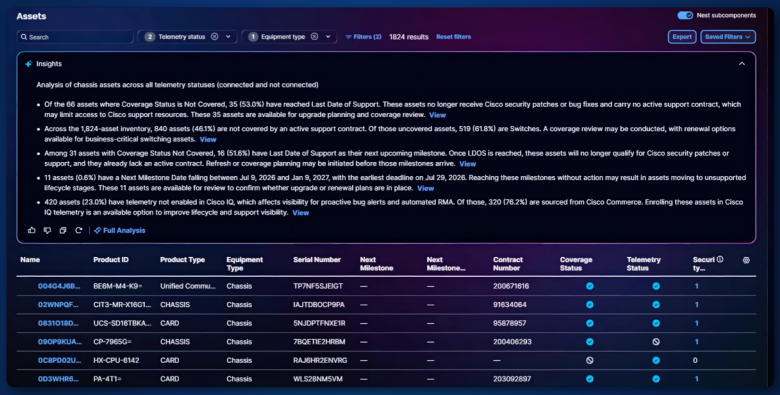
You can't protect what you can't see. Cisco IQ goes beyond basic telemetry-based views. It uses agentic intelligence—built on data from multiple sources, including telemetry, Cisco Support coverage, contracts, hardening guides, and security advisories—to map your entire attack surface by identifying vulnerable assets, assessing hardware and software lifecycle status, and pinpointing the systems that require immediate attention.

It starts by providing a centralized view and management of your Cisco devices, tracking covered and uncovered assets, and mapping them by criticality to prioritize what needs attention and which resources need to be allocated. By monitoring LDOS and overall security health, Cisco IQ enables proactive lifecycle management, helping ensure your network remains secure, compliant, and optimized for peak performance. This isn't a static snapshot; it's an always-on view of your environment.

Map the Attack Surface



Get full visibility of your assets inventory



Exposure Remediation Guidance

Not all vulnerabilities are equal. Cisco IQ correlates security advisories directly with your unique infrastructure, pinpointing which exposures put your most critical assets at risk and demand immediate action, drastically collapsing the discover, assess, and act loop.

What does this look like?

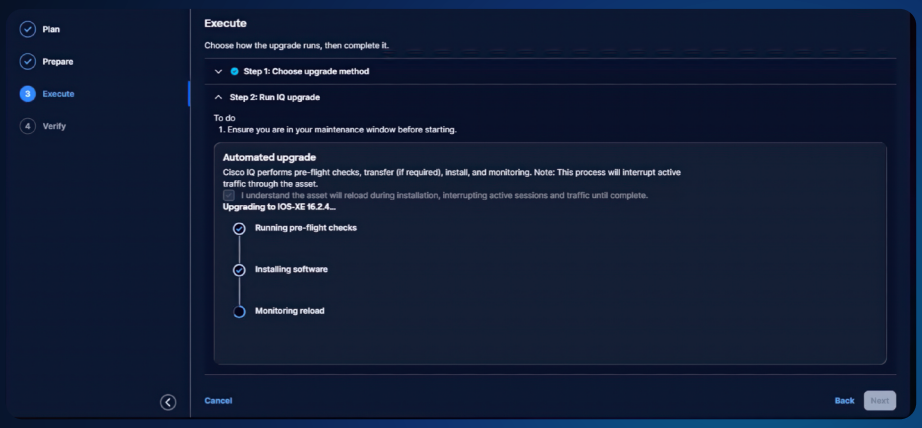
- Assets that can be resolved with an OS upgrade are guided through an automated or manual workflow, including planning for a targeted OS version, verifying and confirming asset readiness, choosing an upgrade method (automated or manual) to run the upgrade, and, lastly, confirming that the version update and upgrade are complete.
- For those assets requiring configuration changes, hardware upgrades, or non-automated OS upgrades, next best actions are identified.

By focusing on what matters most, you can prioritize remediation where it will have the greatest impact on protecting your business.

Remediate Critical Exposures

Identify affected assets

View assets prioritized by criticality and see which ones are upgradable



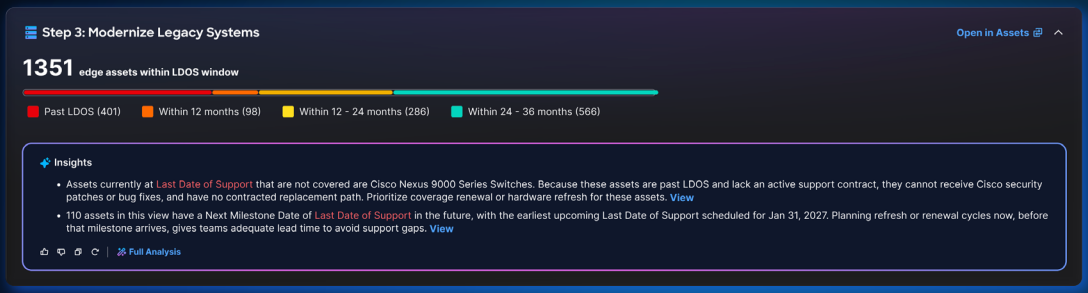
Receive a recommended upgrade path

Modernization Lifecycle Insights

Structural weaknesses—such as flat network architectures and outdated protocols—create entry points for attackers and facilitate east-west movement, transforming isolated security gaps into uncontained blast radii.

These risks are compounded by aging infrastructure, which often lacks the hardware capacity required to meet modern security standards. Cisco IQ identifies devices nearing EoL or LDOS, helping you prioritize modernization planning and engineer resilience into the foundation of your network.

Modernize Legacy Systems



Identify your lifecycle risk

View detailed metrics in the LDOS dashboard

Receive recommended refresh paths for devices near or past LDOS

At a time when the pace and threat sophistication are disrupting business as usual, Cisco IQ provides the AI-powered insights to simplify decision-making and accelerate action. For complex transformations, Cisco Professional Services turn those insights into structural resilience. Cisco de-risks and accelerates your modernization journey by planning and executing critical work—from adopting an Infrastructure as Code methodology and automating deployment pipelines to validating upgrades and implementing dynamic segmentation that contains blast radii. Beyond modernization, Cisco helps you evolve toward an agentic SOC and conduct regular posture-drift reviews, ensuring your defenses remain continuous and hardened through Zero Trust. Move from reactive firefighting to a hardened, always-on, resilient foundation that supports your business with confidence.

Build Resilience at Machine Speed

AI has fundamentally changed the pace of cyber threats. Cisco Resilient Infrastructure Services help organizations respond in kind by combining AI-powered insights, automated workflows, and Cisco expertise to simplify decision-making, accelerate action, and reduce risk with confidence. Powered by Cisco IQ, Resilient Infrastructure Services deliver a personalized, guided experience that helps organizations move from visibility to prioritized action and remediation faster.

Whether you're taking the first step toward greater visibility or modernizing infrastructure for long-term resilience, Cisco helps you move faster from insight to action.

To learn more about Cisco Resilient Infrastructure Services, please contact a Cisco sales representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International
BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**