Cisco Provider Security

In the age of AI, provider infrastructure is critical infrastructure. Cisco helps you keep it secure.

In the age of AI, provider infrastructure is critical infrastructure—and Cisco is uniquely positioned to help providers keep it secure. By integrating AI-native security into the infrastructure itself, Cisco delivers a unified approach that enables providers to protect service delivery, simplify operations, and unlock new revenue opportunities.

Benefits

Establish trust in infrastructure

Protect the integrity of core networks, 5G, and edge with embedded security, trusted silicon, and post-quantum readiness—helping ensure secure service delivery from the physical layer up.

Strengthen threat defense with AI

Stop advanced threats with adaptive, AI-powered defense that protects traffic across domains—including control/user planes, east-west data center traffic, and AI inference pipelines.

Simplify and scale security operations

Unify security, telemetry, and automation across domains to reduce Mean Time To Resolution (MTTR), improve visibility, and free up IT resources for innovation.

Monetize security services

Turn infrastructure security into a business model. Enable managed services—from Distributed Denial-of-Service (DDoS) protection to secure connectivity tiers—powered by built-in Cisco capabilities.

Overview

- Providers power the modern digital world—from AI workloads to multicloud ecosystems, from edge innovation to high-speed global transport. But as you connect more, you're also exposed to more. Threats are faster. Attack surfaces are broader. Trusting your physical infrastructure has never mattered more.

  We help by integrating AI-native security directly into your infrastructure. That means security that scales with you, responds in real time, and creates new opportunities to monetize trusted services.

A Layered Approach to Provider Security

To effectively address today's complex and evolving threat landscape, providers require more than reactive measures or isolated solutions. They need a unified, platform-based security strategy that integrates security into every layer from the outset. Cisco's approach embodies this principle, delivering comprehensive and integrated protection that spans the entire network architecture and aligns with the demands of modern environments.

- **Trusted Foundations**

  Security begins with rigorous validation at the hardware and software levels. Every device is designed to start secure, with strong integrity checks ensuring authenticity and tamper resistance. This foundation establishes the essential trust needed for resilient service delivery.

- **Hardened Systems**

  Security is embedded by default throughout Cisco's products. Continuous efforts to eliminate vulnerabilities ensure that weak points are removed proactively. Cisco delivers solutions that extend security across the network fabric, enabling every component—not just the edge—to contribute to defense.

- **Ready for Quantum**

  Anticipating future threats, Cisco invests in technologies that withstand quantum computing risks. Some products already incorporate quantum-safe protections, ensuring that data intercepted today remains unreadable tomorrow. This commitment goes beyond encryption, maintaining trustworthiness at every system level.

Trends and challenges

Providers (communication service providers such as telco and cable, hosting and application providers, large-scale operators) are transforming. Their networks must scale to meet the demands of hybrid work, multicloud architectures, 5G, and AI—all while supporting distributed users, services, and workloads. With more data processed at the edge (62% by 2027; S&P Global), and AI traffic surging, the attack surface has exploded.

Yet provider networks are often segmented and undervisualized, making the "connective tissue"—from interconnects to VLANs and hybrid clouds—prime targets for attackers like Salt Typhoon and DDoS campaigns. To protect customers and future-proof service offerings, providers must secure their infrastructure from end to end—from silicon to service.

Continuous detection

Cisco's network continuously monitors for threats in real time. Cisco's network telemetry capabilities provide continuous streaming of detailed data from network devices, enabling proactive identification and resolution of network issues and security threats across all environments.

By embedding security into every layer, providers gain the confidence to deliver trusted, innovative services that evolve with the changing threat landscape.

Cisco offers a unified, platform-based approach to provider security that secures infrastructure, streamlines operations, and enables monetizable services. With embedded security, cloud-native innovation, and AI-powered defenses, Cisco empowers providers to protect the entire infrastructure—from silicon to service. This comprehensive strategy equips providers with the security needed to safeguard today's services while adapting to meet the demands of tomorrow.

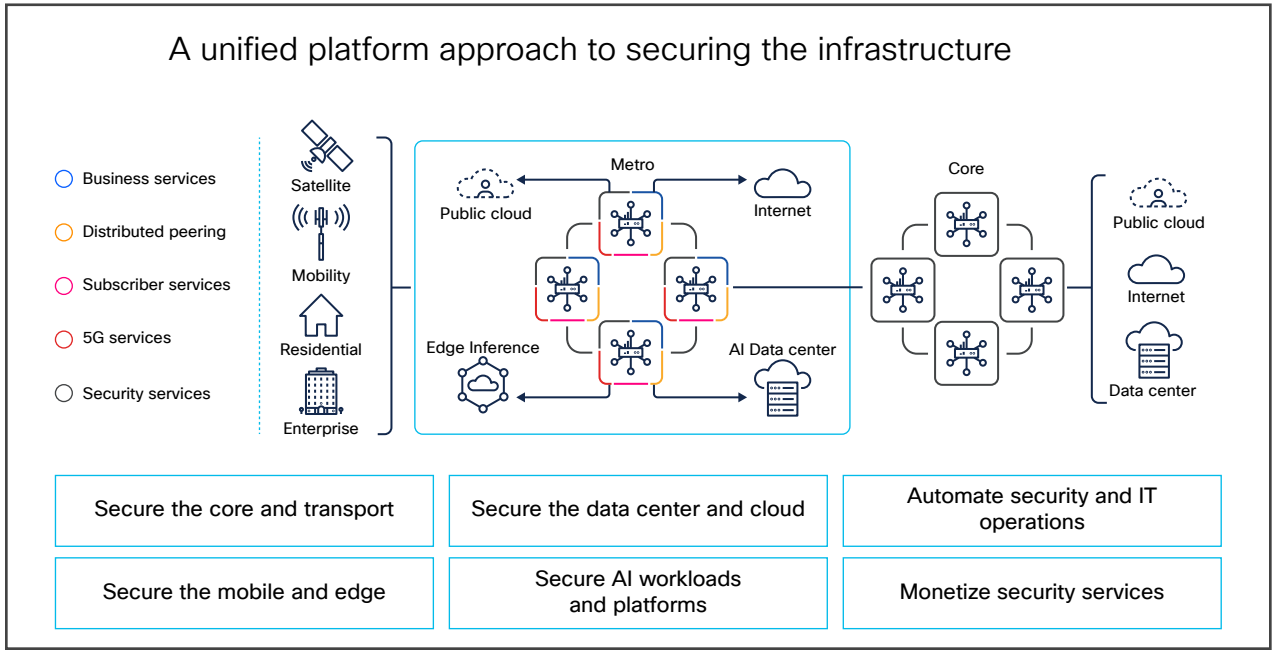

Figure 1. A unified platform approach

Strategic focus areas

To maximize value and deliver real operational outcomes, Cisco takes a unified platform approach to security—focusing on protecting not just isolated components but the vital connective tissue that links every part of the provider environment.

Secure the core and transport network

To safeguard the backbone of provider infrastructure, Cisco embeds advanced security directly into the transport layer. This helps ensure seamless protection for cloud environments, users, and the operational teams responsible for keeping the core secure and resilient.

Secure mobile networks and edge infrastructure

As mobile and edge environments grow in importance, Cisco extends zero trust, DDoS protection, and segmentation out to the network edge. Our solutions protect cloud resources, empower secure user access, and provide the operational visibility and control needed by security operations teams.

Secure the data center and cloud

To defend applications and data moving across data centers and multicloud environments, Cisco provides deep visibility, segmentation, and inline defense. This helps to ensure robust protection for cloud workloads, users, and the operations centers that oversee complex environments.

Secure AI workloads and platforms

With AI workloads proliferating at the edge and in the cloud, Cisco delivers real-time detection and embedded security to keep inference pipelines and platforms safe. Our integrated solutions protect cloud-based AI, secure user interactions, and enable effective monitoring and rapid incident response.

Automate security and IT operations

Operational efficiency and rapid response are critical at scale. Cisco's automation and analytics platforms empower teams to detect, enforce, and respond to threats across domains while maintaining a strong security posture for cloud assets and users.

Monetize security services

Providers can transform embedded security into revenue-generating managed offerings. Cisco's platform makes it easy to package and deliver premium protection for cloud services, end users, and the operations teams that support them.

"Providers must secure their infrastructure from end to end—from silicon to service—to protect customers and future-proof service offerings as hybrid work, multicloud, 5G, and AI expand the attack surface across distributed environments."

Use cases

Table 1. Use cases by industry

Industry	Use cases
CSPs (telcos/cable)	Secure 5G, broadband, and core transport networks with end-to-end visibility, automated threat response, and embedded security. Cisco's unified platform approach protects subscribers, helps ensure uptime, and supports new managed services—enabling CSPs to adapt quickly while monetizing secure connectivity in fast-evolving hybrid and AI-driven environments.
Media companies (Paramount, Disney, etc.)	Safeguard streaming platforms, content distribution, and production workflows with layered security and automated defenses. Cisco protects media assets from piracy, DDoS, and data breaches while enabling secure remote collaboration and cloud workflows—helping ensure seamless content delivery and audience trust, even as digital and AI-powered experiences expand.
Webscalers/neocloud (AWS, Google, etc.)	Defend hyperscale cloud environments and multitenant services with integrated, AI-powered security and real-time analytics. Cisco's platform safeguards massive traffic volumes, supports compliance, and automates threat response—empowering webscalers to deliver secure, differentiated cloud offerings while protecting workloads and user data across global, distributed infrastructure.
Large-scale operators (hosting, federal and defense, global finance)	Protect mission-critical applications and sensitive data with unified security, granular segmentation, and automated compliance. Cisco enables large operators to secure hybrid, edge, and on-premises environments—minimizing risk, helping ensure regulatory adherence, and empowering innovation for hosting providers, government agencies, and global financial institutions in an ever-evolving threat landscape.

"Cisco delivers a unified, platform approach to provider security—embedding security into every layer, enabling trusted, innovative services and allowing providers to defend against evolving threats while monetizing new opportunities at scale."

Enabling secure service delivery and revenue growth with Cisco CX

Cisco Customer Experience (CX) delivers vital support to Providers as they implement and grow their security offerings. Leveraging Cisco's deep expertise, Providers can optimize every stage of their security journey—ensuring their networks remain secure, reliable, and scalable. Cisco CX guides Providers through assessment, planning, deployment, and optimization, enabling the seamless integration of advanced security technologies such as threat detection, firewalls, and network segmentation. With proven methodologies and proactive strategies, Cisco CX helps Providers reduce security risks, protect sensitive data, and maintain compliance with industry regulations. Through expert guidance and operational support, Providers can accelerate time-to-market for new security services and products, staying ahead of industry demands. Cisco CX also provides expert incident response capabilities, helping Providers quickly identify, contain, and remediate security incidents, which enhances readiness, minimizes impact during breaches, and supports continuous improvement of security posture. Additionally, Cisco CX assists Providers in designing tailored, value-added security service packages for their end customers, creating new revenue streams and business opportunities. By leveraging Cisco CX's ongoing support and insights, Providers can deliver high-quality security services, differentiate themselves in the market, and foster lasting, trust-based relationships with their clients.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

With Cisco, providers can

- Secure their entire service delivery chain, including interconnects.
- Defend against emerging AI and nation-state threats.
- Simplify and scale SOC/NOC operations with automation.
- Launch new security-backed services with confidence.

Trusted partners in the age of AI

Cisco enables providers to protect their infrastructure, grow revenue through secure offerings, and become trusted, resilient partners ready for the AI era and whatever comes next.

The Cisco Advantage

For over 40 years, Cisco has been building and securing the global internet. Our infrastructure powers over 76% of the networking market, and we secure 100% of the Fortune 100. Cisco is trusted by the largest providers, enterprises, and governments on earth. Unlike vendors who bolt on technology as an afterthought, Cisco is integrating AI-native, adaptive security directly into the infrastructure service providers already run—across routing, switching, cloud, and edge. With innovations like Hypershield, Cisco Talos® threat intelligence, and post-quantum crypto readiness, we deliver platform-level security built for speed, scale, and complexity of critical infrastructure.

- Trusted by 100% of Fortune 100 for security (Cisco Newsroom).
- Powers over 76% of global networking infrastructure (Examsnap 2025 market analysis).
- Integrates security across routing, switching, and interconnect—not “bolted on”.
- Provides AI-native protection for AI-generated threats and AI workloads.
- Offers visibility across the full-service delivery chain—including interconnects.
- Designed for provider performance, scale, and monetization models.
- Powered by Talos—one of the largest commercial threat intelligence teams in the world.
- Future-ready to protect from tomorrow’s threats by addressing post-quantum cryptography requirements now—with tools built directly into the stack (Session Key Service [SKS], Secure Key Integration Protocol [SKIP]).

Learn more

Ready to transform your provider infrastructure into trusted, resilient, and revenue-generating critical infrastructure? Discover how Cisco’s unified, platform approach to security can help you lead with confidence. Contact us to get started today. https://www.cisco.com/site/us/en/solutions/service-provider/security/index.html.

C22-5650351-00 01/26