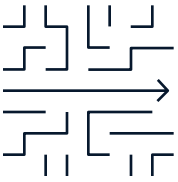
Galvanizing Service Provider Resilience in the AI Era

Introduction: The 8-hour reality

The clock is ticking. According to Cisco's analysis, the window between the discovery of a vulnerability and the emergence of a weaponized exploit is expected to collapse from approximately 2.3 years in 2018 to a mere 8-hours in June 2026. This rapid escalation is compounded by the persistent risk of aging infrastructure. According to the Cisco Talos Intelligence 2025 Year in Review, 40% of vulnerabilities directly impact End-of-Life (EOL) devices, and 32% of vulnerabilities are at least a decade old. We have entered the AI era, which requires organizations to implement security capabilities that function at AI speed and scale while simultaneously adopting an operating model that supports a continuous approach to cyber defense. This transition represents both a necessary evolution in technical capabilities and a fundamental organizational shift.

As an early member for Anthropic's Project Glasswing and OpenAI's Daybreak, Cisco® is leveraging direct, early access to Claude Mythos Preview and GPT-5.5-Cyber models. This collaboration enables us to identify and remediate issues in existing codebases and enhances our software development lifecycle to prevent, detect, and respond to threats.

For Communications Service Providers (CSPs), current operating models are insufficient to address this landscape. To survive and thrive, CSPs must accelerate their architectural transformation toward simplified, autonomous networks. This paper outlines the three pillars of this transformation: Network Simplification, Automated Software Hygiene, and the fortification of the CSP's own Enterprise Landscape.



Pillar 1: Network simplification

Network complexity invariably creates expanded attack surfaces. By reducing the number of nodes and streamlining processes, the network posture becomes a manageable challenge. The following architectural changes are crucial to lower the complexity, while reducing the threat surface at the same time.

Segment Routing (SR): The foundation of simplicity

While Segment Routing (SR) is widely celebrated for its ability to elegantly "slice" networks into strict, assurable SLAs, its primary original driver was radical simplicity. By reducing the protocol stack from four to one, SR drastically shrinks the network's attack surface.

SR's slicing capability provides the critical platform for service convergence, enabling the retirement of complex legacy networks even in diverse environments. A prominent example is Swisscom, which successfully converged 20 disparate networks into a single SRv6 platform. This move not only enabled assured end-to-end (e2e) services but also significantly reduced the threat surface while future-proofing the infrastructure for the rigorous demands of proliferating AI traffic over the WAN.

A key by-product of this modernization is the systematic removal of vulnerable, End-of-Support (EoS) systems—software that can no longer be patched or upgraded and often lacks modern protections such as memory safety mechanisms and exploit mitigations. To accelerate this process, you can use the Cisco IQ platform to quickly uncover unsupported hardware and software across your estate. Furthermore, these modernized platforms natively support post-quantum cryptography, ensuring your customers' valuable data remains protected today, even as we prepare for tomorrow's quantum-computing world.

Control User Plane Separation (CUPS) and aaS

Mobile and wireline subscriber management are inherently complex, particularly from a control plane perspective. Cisco has found that by centralizing this control plane complexity, the distributed user planes—which enable traffic breakout closer to the subscriber—operate on a significantly simpler software stack.

Broadband Network Gateway with Control and User Plane Separation (CUPS BNG) modernizes the subscriber edge through control and user plane separation, giving operators a more agile, scalable, and operationally simple architecture. Wireline subscriber management is inherently complex, particularly in the control plane, where subscriber state, policy, authentication, Operations Support Systems/ Business Support Systems OSS/ BSS integration, and service logic must be managed at scale. By centralizing this complexity into a cloudified, microservices-based control plane, operators can scale the Control Plane and User Plane (CP and UP) independently, apply CI/CD-based lifecycle management, and enable drastically simplified, hitless control-plane upgrades. This is increasingly important in the era of AI-driven operations, where rapid issue resolution, including AI-era fixes, must be delivered quickly, securely, and without subscriber downtime.

At the same time, CUPS enables distributed user planes to be placed closer to subscribers for edge offload, improving performance while reducing unnecessary backhaul. Because the UP no longer carries subscriber state or direct OSS/northbound dependencies, it runs on a significantly simpler software stack, driving approximately a 40% reduction in user-plane software complexity. This simplification lowers operational risk, makes UP upgrades safer, and reduces the blast radius of changes compared to an integrated BNG model. With session steering, operators can create and introduce new services faster, direct traffic to the right user-plane location, and better align compute and forwarding resources to demand for a right-sized footprint. Overall, CUPS BNG delivers elastic scale, service agility, simplified upgrades, edge offload, and unified subscriber management across access types such as Gigabit Passive Optical Network (GPON), 10Gbps symmetrical PON (XGS-PON), and Fixed Wireless Access (FWA).

Given the inherent additional complexity of the Mobile Packet Core, Cisco offers this function as a Service (aaS). This model allows for compliance with strict sovereign requirements—for example, hosting the control plane within an EU jurisdiction (such as Frankfurt) while managing the user plane locally (such as Milan). By delivering this as a service, Cisco applies its deep expertise in Kubernetes security, implementing extended Berkeley Packet Filter (eBPF) at multiple levels of the stack to maintain a razor-sharp focus on software hygiene.

Layer convergence and SoC

Collapsing the Optical layer into the Routing/Switching layer through highly efficient, standard form-factor coherent pluggable optics adds an extra dimension to convergence and hence simplification. Power Savings of upto 85% - as recently confirmed in Deutsche Telekom's deployment of Routed Optical Networking – are catalysing mainstream deployments. And now another emerging benefit is that by removing yet another layer of devices, and the code that runs upon them, will natively reduce the threat surface further.

System-on-a-Chip (SoC) designs

Taking advantage of System-on-a-Chip (SoC) designs—where SerDes from highly scalable, right-sized NPUs provide direct connectivity to router interfaces—offers significant benefits across multiple vectors. By negating the need for additional power-hungry and costly components such as fabric cards and redundant memory modules found in traditional designs, we reduce hardware complexity. This reduction in physical components inherently lowers the software overhead required to manage them, which in turn helps mitigate potential failure rates and reduces the overall threat surface.

While modular platforms remain a cornerstone of our portfolio and continue to provide essential support for high-capacity, high-density environments, the industry is increasingly adopting SoC-based designs to achieve greater efficiency in specific deployment scenarios.

Resilient architectures

Beyond the hardware itself, we must revisit network architectures optimized for both resilience and cost. Modern network design is shifting toward smaller failure domains, which limits the "blast radius" of any single incident and restricts the potential for lateral movement by threat actors.

This is now more achievable than ever through simpler platforms and increased layer convergence. By investing in dual-homing strategies whenever possible, we enable the ability to take individual components offline for maintenance or upgrades without causing major service disruption. When these simplified systems are combined in physically redundant, fabric-type architectures, the uptime of the overall network is drastically enhanced. Crucially, because these individual chassis can be serviced without affecting live traffic, fleet-wide software upgrades become far simpler and can be performed with greater frequency. This shift in architectural thinking is a fundamental enabler of our next subject: holistic Software Hygiene.

Pillar 2: Software hygiene and runtime security

Operating system vulnerabilities are increasingly discovered and exploited at machine speed. This shift fundamentally changes the requirements for patch management and necessitates new approaches to defend against zero-day threats. Both challenges must be addressed holistically as part of a modernized, automated software hygiene operation.

Zero-day threats and Live Protect

Manual patching cycles cannot keep pace with the velocity of modern critical vulnerabilities, nor is it operationally feasible for CSPs to execute such frequent, disruptive upgrades. In the interim, we can deploy compensating controls to isolate vulnerable processes. By deploying an eBPF-based agent within the operating system kernel, Cisco can rapidly protect systems without impacting CPU performance or risking network downtime.

This solution, Live Protect, is available today for the Cisco Nexus Data Center Networking family and Enterprise Routing (Cisco IOS XE) and is currently under development for XR Routing platforms. This provides a clear path to end-to-end zero-day protection—from applications running in a secured data center, through the WAN and its last mile, and into your managed enterprise Customer Premises Equipment (CPE).

While outside the primary scope of this paper, it is worth noting that eBPF is also a foundational component of the Isovalent and Cisco Hybrid Mesh Firewall. These solutions work in tandem to extend firewall protection to top-of-rack switch ports and directly into the host kernel itself.

Full software patching

Upon the release of a software patch, the primary challenge is the typically lengthy—often multi-month—testing cycle required by CSP operations before deployment. Cisco addresses this by applying machine learning and advanced services to drastically shorten these validation cycles.

The role of software fleet management solutions becomes increasingly critical in this process. When combined with fabric architectures, these solutions enable the rapid deployment of non-traffic-impacting software upgrades, effectively negating the traditional requirement to wait for a strictly planned maintenance window. This holistic approach—encompassing both zero-day compensating controls and rapid software deployment—should be managed under the umbrella of a uniform Software-Defined Networking (SDN) controller, as depicted below.

Pillar 3: Securing the operational enterprise

Securing the organization that operates the network

While this paper has focused on the Service Provider's core mission—embedding security into network infrastructure to provide resilient services to customers—there is an often-neglected area critical to overall resilience: the internal enterprise network. Ensuring the uptime of this network is essential for keeping operations teams online, but it also represents a significant attack vector. If compromised, it serves as a gateway for threat actors to infiltrate customer data or gain privileged access to the production infrastructure.

Cisco Cloud Control serves as a unified operations platform for the entire enterprise estate. By converging identity (including that of AI agents), topology, and policy across networking, security, and observability domains, it enables the management of critical infrastructure from a single environment. This shift moves beyond passive monitoring to active execution, enabling real-time defense and streamlined operations—including fleet-wide software upgrades and configuration consistency—all within a governed control path.

This centralized approach reduces complexity, allowing your teams to maintain a cohesive security posture across the entire internal network.

Final thoughts

In the AI era, security is no longer a feature but a core operating model. By embracing and accelerating network simplification, autonomous software hygiene, and unified enterprise control, Service Providers can transform their infrastructure into a resilient, proactive platform capable of defending against the most sophisticated AI-era threats. Cisco is committed to this holistic journey—protecting your managed enterprise CPE, across the WAN into your hosted applications, and indeed your own enterprise environment—applying the expertise and the AI-powered tools necessary to secure the world's critical infrastructure.

C11-6530827-00 08/26