Cisco IOS XE 16: Secure, Open, and Flexible

Cisco IOS XE software operating system for an entirely new era in networking

Digital transformation is affecting businesses and organizations on a massive scale. IT and business leaders are trying use the power of digital technologies to improve business efficiency without having to replace their existing infrastructure.

IT and business leaders are looking for open and extensible platforms that can allow customer applications and third-party applications to integrate with Cisco® devices. They are trying to automate and orchestrate network changes to reduce OpEx using standard APIs, then providing a consistent customer experience with simpler device management and faster troubleshooting and lowering the cost of keeping the network updated.

Benefits

- **Open:** Standards-based capabilities on Cisco network devices accelerate business and network innovation.

- **Programmable:** Programmable interface enables process and workflow automation.

- **Secure:** End-to-end security and trust are built in.

- **Modular:** Modular software independently upgrades individual software modules.

- **Common software stack:** Reduces business and network complexity, allowing you to qualify and deploy new service more quickly.
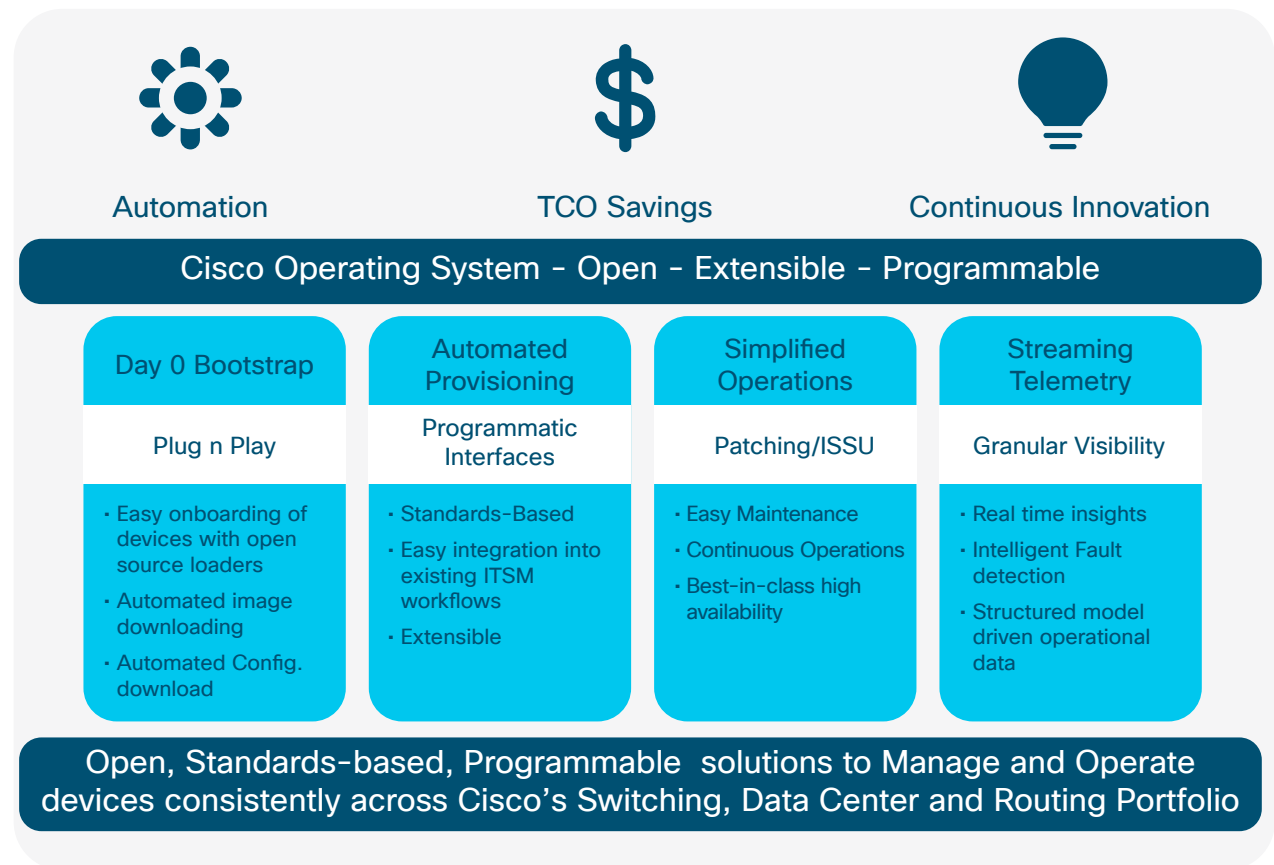
Sophisticated automation

Cisco IOS XE 16 is designed to enable you to do more tasks in less time and provides consistency across Cisco switching, routing, and wireless network devices that learns from information from across the network to create a simpler, more fluid experience. This intuitive network can automate mundane day-to-day operations, which shifts IT time and money to focus on creativity and design.

Transformational magic

Cisco IOS XE continually evolves and transforms to anticipate customer needs with exponential results, creating and driving new industries and fostering innovations that have yet to be envisioned.

Cisco IOS XE: Open, Programmable, Secure

Cisco IOS® XE has been designed to allow you to deploy services more quickly with lower TCO and minimized complexity. Cisco IOS XE 16, combined with Cisco DNA™ Center and Software-Defined Access, can reduce training and upgrade time, simplify qualification, speed testing and device monitoring, and improve network operations with a consistent OS across access, distribution, core, wireless, and WAN.

Automation	TCO Savings	Continuous Innovation

Cisco Operating System - Open - Extensible - Programmable

Day 0 Bootstrap	Automated Provisioning	Simplified Operations	Streaming Telemetry
Plug n Play	Programmatic Interfaces	Patching/ISSU	Granular Visibility
· Easy onboarding of devices with open source loaders · Automated image downloading · Automated Config. download	· Standards-Based · Easy integration into existing ITSM workflows · Extensible	· Easy Maintenance · Continuous Operations · Best-in-class high availability	· Real time insights · Intelligent Fault detection · Structured model driven operational data

Open, Standards-based, Programmable solutions to Manage and Operate devices consistently across Cisco's Switching, Data Center and Routing Portfolio

Built-in security protection

At Cisco, security is our top priority. To protect against today's cyberthreats, we take a holistic approach to security that includes building security into every facet of our business. We've committed to ongoing investment, innovation, and industry leadership in the rapidly evolving security market. In addition to offering industry-leading security products and services, Cisco is building in security and trust across our solutions portfolio. That includes switches, routers, servers, and cloud solutions.

Our approach is much more than just adding security as an afterthought to existing products. It's about embedding security into the essence of our products during the design phase. The result is that security is a primary design consideration, deeply integrated into the underlying architecture.

This built-in security provides platform integrity, facilitates secure communications, guards against counterfeit products and tampering, gives customers confidence that their Cisco products are genuine and unmodified, and helps make sure that the data coming from your Cisco infrastructure can be trusted. These features have positive compliance implications for our customers. For example, validation of a digital signature on the Cisco IOS Software installed on a platform is evidence that an auditor can use to state that the software on that platform is genuine and unmodified. This validation is done when a platform is started up and can be done against the running Cisco IOS copy on customer demand with a simple Command-Line Interface (CLI) command.

Primary features

Table 1.   Primary features

Modularity	• Processes can be statefully upgraded/restarted without taking device down. • Features can be deployed and rolled back in minutes without changing the underlying software image.
Openness and programmability	• NETCONF (RFC 6241) enables integration with SDN controllers and configuration management tools. • RESTCONF (RFC 8040) provides a standards-based programmatic interface for accessing configuration data, state data, data-model-specific for YANG models. • IETF YANG push telemetry permits analytics tool (for example, ELK Stack) integration. • OpenConfig and IETF YANG data models deliver easy integration into heterogeneous network environments. • Guest Shell Linux Containers (LXCs) securely host third-party Linux applications. • Preboot execution and Cisco network plug-and-play clients along with zero-touch provisioning automate Cisco network device deployment. • YANG data models automate Cisco network device configuration management through DevOps tools such as Ansible and Puppet. • Python scripting and custom libraries automate event-based workflows on Cisco network devices.
Debuggability	• Always-on binary tracing captures all the runtime interaction all the time to allow full. • Lightweight binary tracing, enabled through the compiler, allows always-on tracing so that all states for all time can be captured. • Radioactive tracing specifically targets areas where the system has failed.

More information

For more information about Cisco IOS XE, visit www.cisco.com/go/ios.

For more information about Cisco IOS XE programmability, visit https://developer.cisco.com/site/ios-xe.

For more information about Cisco switches, visit www.cisco.com/go/switching.

For more information about Cisco routers, visit www.cisco.com/go/routinging.

Cisco IOS XE 16.x platforms supported

Table 2.   Supported platforms

	Products Supported by Cisco IOS XE 16.x
Controllers	Cisco Catalyst 9800 Series Wireless Controllers
Switches	Cisco Catalyst® 9500, 9400, 9300, 3850, and 3650
Aggregation/edge routers	ASR1013, ASR1009-X, ASR1006-X, ASR1006, ASR1004-X, ASR1002-HX, ASR1001-HX, ASR1002-X, and ASR1001-X
Branch routers	4451 ISR, 4431 ISR, 4351 ISR, 4331 ISR, 4321 ISR, 4221 ISR, and 1000 ISR
Virtual routers	CRS 1000v, ISRv