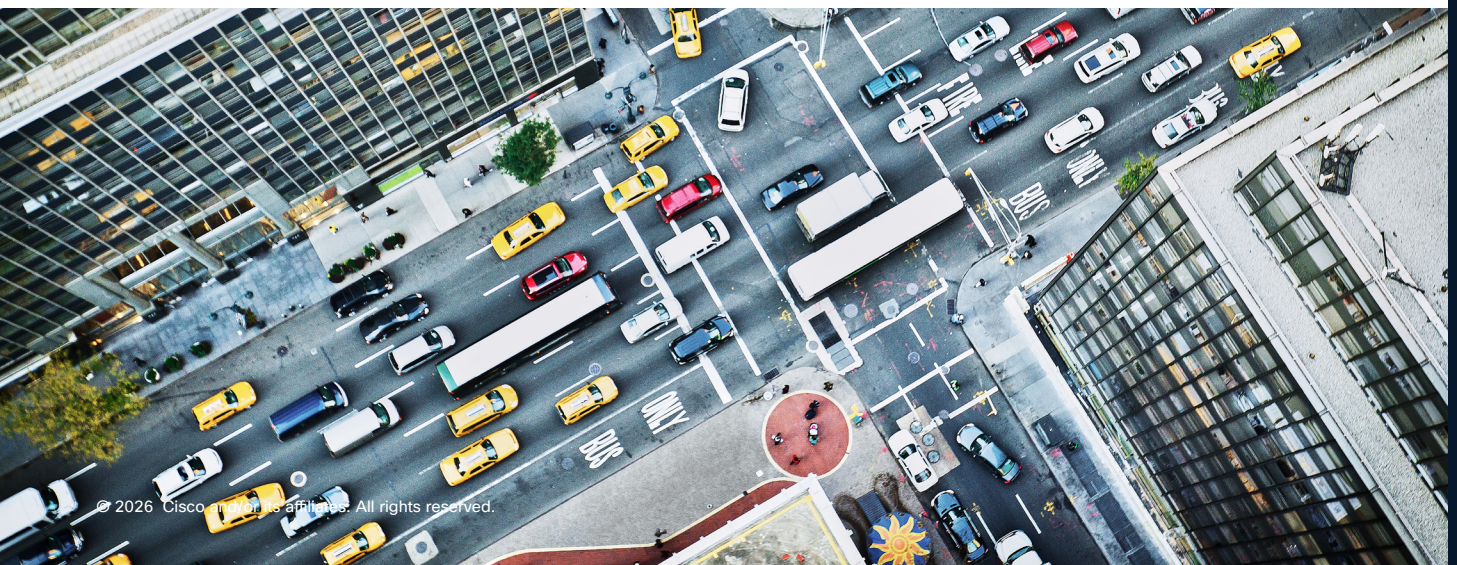
Robust Cybersecurity to Safeguard Roadways Infrastructure

Roadway operators are at a crossroads: they must connect an ever-increasing array of field assets, such as traffic signal controllers, remote weather stations, cameras, variable message signs, or pedestrian detectors to help reduce traffic congestion, limit carbon emissions, and improve public safety.

The pressure to deploy AI-driven traffic management and Intelligent Transportation Systems (ITS) as well as protecting these critical infrastructures against escalating cyberthreats render legacy, siloed networks obsolete. By combining a market-leading portfolio of rugged networking equipment and a comprehensive range of cybersecurity solutions, Cisco offers a powerful architecture to build modern and secure connected roadways.



Benefits

- Build a secure WAN with comprehensive threat detection, protection, and response capabilities.
- Drive cyber hygiene with deep visibility into connected assets and your security posture.
- Control third-party access to devices with zero-trust remote access built into the infrastructure
- Reduce the risk of unauthorized access to field network equipment.
- Keep attacks from spreading by enforcing dynamic network segmentation.
- Easily manage assets connected over cellular networks.

© 2026 Cisco and/or its affiliates. All rights reserved.

Build a robust and highly secure WAN infrastructure to connect all your roadside assets

The distributed nature of roadway infrastructures requires a complex network spanning multiple locations. The Cisco SD-WAN solution with Cisco industrial routers is ideally suited for these demanding requirements. It combines enterprise-grade performance and security with industrial-strength reliability and resilience.

Unify security policies to defend against threats

Cisco industrial routers offer comprehensive Next-Generation Firewall (NGFW) and network security features. Catalyst™ SD-WAN Manager centralizes routers and security configuration to unify security policies, eliminate gaps in defense, and simplify managing and securing roadway infrastructures at scale. Build a modern and secure WAN with Cisco industrial routers and these embedded security features:

- **Next-generation firewall** with application awareness to filter traffic in real time and provide granular control capable of detecting thousands of applications.
- **Intrusion detection and prevention (IDS/IPS)** with Talos® signatures to identify and block known threats and malicious activities such as vulnerability exploits.
- **Advanced malware protection** to identify and block both known and unknown threats from malicious files. Unknown files can be sent to a sandbox for further analysis.
- **URL filtering** to block or allow users to access URLs based on reputation or web categories covering millions of domains and billions of web pages.
- **DNS security** to prevent infected assets from contacting malicious servers.

There's a rugged router for every need

In addition to advanced network security features, Cisco industrial routers offer unconditional connectivity for all your roadside equipment. They can withstand extreme temperatures, humidity, and dust. They offer a variety of WAN connectivity options, including 4G/5G cellular, MPLS, Ethernet, and fiber, through pluggable interface modules that can easily be replaced when needs or technologies evolve.

Cisco Catalyst IR1100 Rugged Series Routers



A compact, modular, and expandable router that fits in any cabinet to securely connect ITS assets.

Cisco Catalyst IR1000 Rugged Series Routers



An ultra-compact, low-power router built for space-constrained cabinets and sites powered with solar panels and batteries.

Cisco Catalyst IR1800 Rugged Series Routers



This modular router offers multiple cellular interfaces, Wi-Fi 6, and advanced SD-WAN security capabilities.

For more information on Cisco industrial routers, visit cisco.com/go/iot-routers

© 2026 Cisco and/or its affiliates. All rights reserved.

Gain visibility into your roadway assets

Securing your roadway assets starts with having an accurate and detailed inventory of what's connected. Knowing what you have, and continuously updating the list, is the first step to efficiently manage resources and drive security hygiene to reduce the attack surface.

Cisco® Cyber Vision identifies all your assets and uncovers the smallest details: device types, vendor references, serial numbers, firmware and software versions, and more. You can now build a plan to improve your security posture and drive compliance with security regulations.

Visibility you can easily deploy at scale

Cyber Vision embeds visibility capabilities into Cisco industrial routers and switches installed at intersections, in street cabinets, along highways, or in your control center. It analyzes every IP packet moving into or out of your ITS devices without the need for additional security appliances and the effort of installing them. Your network is the sensor and sees everything that connects to it to save on WAN costs and enable deployment at scale.

Visibility that meets you where you are in your journey

Whether you just need to assess your security posture to drive improvements or you're ready to enforce advanced security policies, we've got you covered. Cyber Vision automatically profiles connected assets and maps their communications. It feeds your cybersecurity tools with ITS context so you can protect your infrastructure by easily creating access control policies. It monitors ITS communications so you can detect, investigate, and remediate threats using your IT security tools.

For more information on Cisco Cyber Vision, visit cisco.com/go/cybervision.



© 2026 Cisco and/or its affiliates. All rights reserved.

Apply a zero-trust policy to your infrastructure

Because your network equipment is installed in street and road cabinets, you need robust security, starting where the roadway devices physically connect. Zero-trust security principles must be implemented to ensure that bad actors cannot connect to your network in case they gain access to the cabinets. All communications should be monitored to continuously verify trust and isolate devices that have been compromised. This is particularly important in roadways, since the ITS protocols typically do not have Transport Layer Security (TLS), and key information/credentials are sent in plain text.

Cisco industrial network equipment combined with Cisco Identity Services Engine (ISE) and Cisco Cyber Vision offers a simple and powerful way to define and enforce zero-trust policies across your roadways infrastructure.

Ensure that only your roadway assets can connect

Securing every port of your field networking equipment is key. Cisco ISE manages network access using IEEE 802.1X or MAC Authentication Bypass (MAB) to help ensure that only the devices you specify are granted access. Combined with Cyber Vision, the solution is even simpler to implement. The assets you trust are identified by Cyber Vision and the list is dynamically shared with ISE. All other devices are denied access by default.

Enforce trust through network segmentation

Once a device is granted access, you need to ensure that it communicates only with the resources it needs to do its job. Security policies must be enforced to build zones of trust for each device as defined in the IEC-62443 security standard. As it tracks all assets and their activities, Cyber Vision can automaticallys suggest and enforce policies that segment the network according to your operational constraints.



For more information on how to secure distributed field networks, check out our solution brief.

© 2026 Cisco and/or its affiliates. All rights reserved.

Enable easy-to-use, secure remote access

Your roadway assets are distributed across your city, region, or country. Enabling remote access is key to eliminate truck rolls, reduce costs, and minimize downtime. Whether you need to grant access to third parties or make it simple for your technicians to manage assets connected over cellular networks, you want a remote access solution that's easy to implement and highly secure.

Cisco Cyber Vision turns your Cisco industrial routers and switches into remote access gateways, so there is nothing extra to install in space-constrained roadside cabinets. It's a cloud service, so it's very easy to deploy, configure, and scale. And it's a security solution, so it lets you control who can access what, when, and how.

Remote access made for operations

Cyber Vision is the ideal remote access alternative to punching multiple holes in firewalls or configuring port forwarding in from the public internet. Users have access only to the devices they need to service. Multi-Factor Authentication (MFA) can be enforced, and you get full audit logs to track who did what.

Operations managers can create remote access credentials by themselves to immediately enable access when needed. Yet security policies are always enforced. Logging into remote assets simply requires a web browser, but desktop applications can also be used for advanced management tasks. All without having to install additional appliances in remote sites.



For more information on Cyber Vision's secure remote access capabilities, visit cisco.com/go/cybervision.

© 2026 Cisco and/or its affiliates. All rights reserved.

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.



Secure your roadways infrastructure with Cisco

Talk to a Cisco sales representative or channel partner and visit cisco.com/go/connectedroadways or cisco.com/go/iotsecurity to learn more.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C22-3731723-03 10/26