Cisco

The Importance of Cyber Security in the Rail Industry

The railway industry is increasingly embracing new systems and technologies to enhance operational efficiency, safety and connectivity.

As operators move on from their legacy systems, there is an ever-increasing number of connections and complexity to deal with from a security standpoint.

Expanded connectivity means increased chances for cyber criminals to disrupt critical infrastructure and global economies. Threats have gone from simple hacks to sophisticated attacks for financial gain, disruption and espionage. The world's critical infrastructure – power grids, healthcare systems, food industries and transportation – can and have been disrupted by cyberattacks.

At Cisco, we're listening and working alongside rail operators, governments and our networks to map out a digital future with trust at its foundation.

Enterprise Architecture Approach

An enterprise architecture approach and zero trust

framework is recommended to think more holistically about how components in a network can work together to drive security and operational resilience. This enterprise approach, versus one that is more siloed, can deliver enterprise segmentation, security and compliance across the ecosystem.

Collecting and analysing telemetry at the lowest granular level provides the comprehensive visibility needed to enable rail operators to see what's going on on their network – in real time. This level of visibility enhances the capacity to troubleshoot whether the network is undergoing network performance issues or facing an adversarial attack. Visibility and analytics also result in the ability to orchestrate a dynamic response to either – anywhere across the enterprise.

Cisco Connected Rail

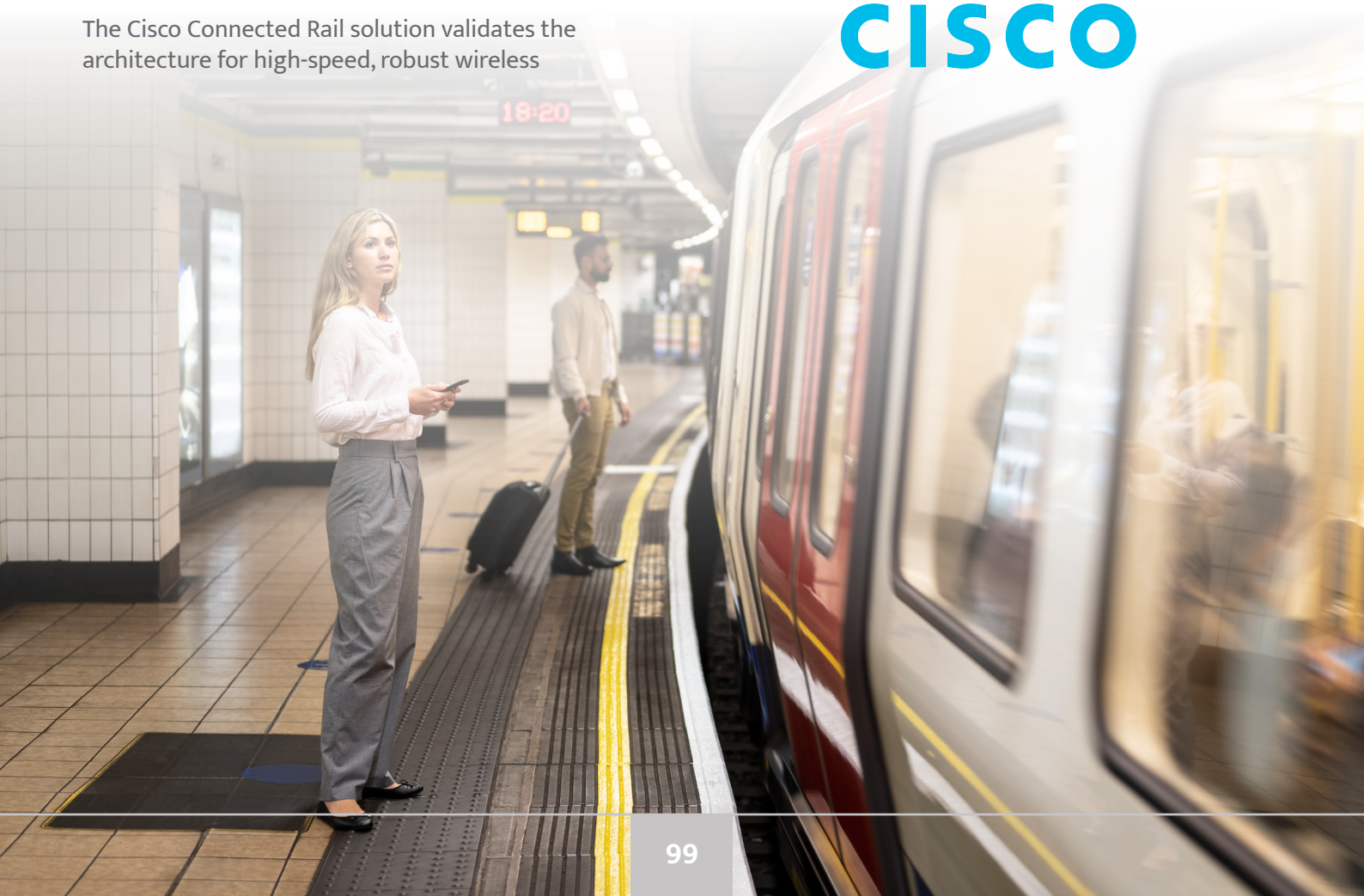
The Cisco Validated Design for Connected Rail provides an end-to-end architectural framework and a resilient network foundation designed to improve the safety, efficiency, performance and service levels of rail operations. This architecture includes network segmentation to securely deliver multiple services (vital and nonvital) over a common infrastructure – lowering risk and reducing cost.

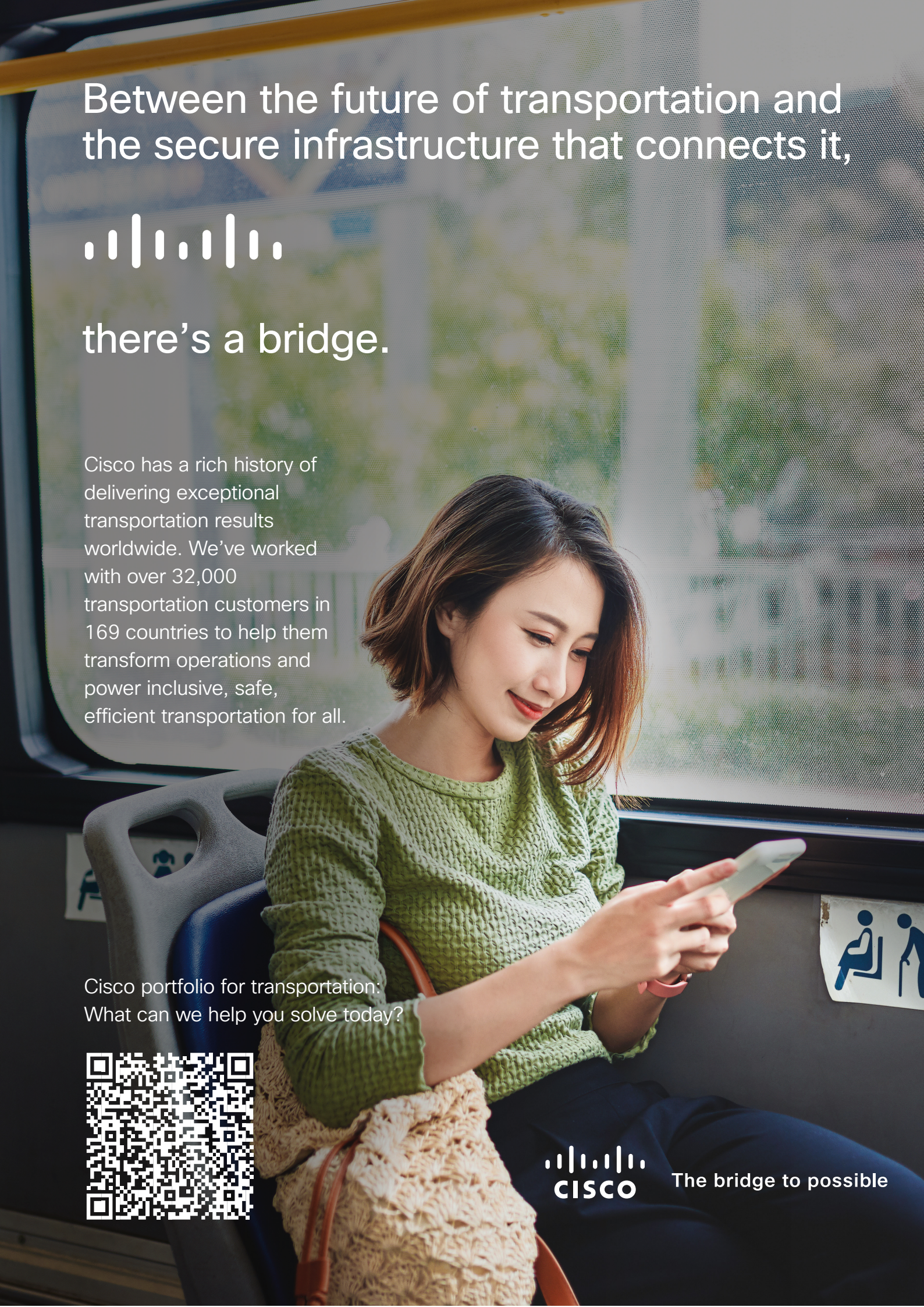
The Cisco Connected Rail solution validates the architecture for high-speed, robust wireless connectivity between train and trackside as well as resilient, scalable access and backhaul transport infrastructure to interconnect wayside, stations and operations centres across an operator's regions.

Simplified Approach to Security

The new digital reality that rail operators face brings with it an unprecedented level of risk. The volume and sophistication of threats have left these organisations with a mixture of security tools that don't always work together, are unnecessarily complex and aren't well-suited to address increasingly advanced and costly attacks.

Cisco works with rail operators around the world to achieve a holistic, simplified approach to security, privacy and trust. At the heart of our approach is integration – reducing the complexity of managing dozens of products. With this platform approach, customers work seamlessly with the tools they have to create a more safe and secure transportation ecosystem.




Between the future of transportation and the secure infrastructure that connects it,
there's a bridge.
Cisco has a rich history of delivering exceptional transportation results worldwide. We've worked with over 32,000 transportation customers in 169 countries to help them transform operations and power inclusive, safe, efficient transportation for all.
Cisco portfolio for transportation:
What can we help you solve today?
CISCO
The bridge to possible