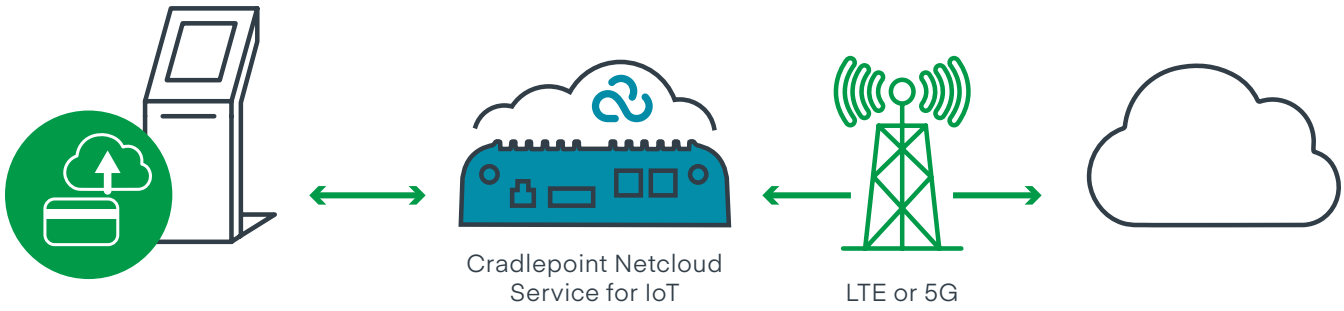
Interactive Kiosks for Shopping and Services

Using LTE and 5G to deliver point-of-sale and other applications

Companies in virtually every industry now use kiosks to make their services much easier to access. Many of these kiosks accept credit card payments, which is very convenient for customers, but also challenging for IT teams. They need the agility to move their kiosks multiple times without constantly ordering new wired lines, and without having to manage and troubleshoot connectivity in person. Perhaps most importantly, they must have assurance that their customers' payment information is protected at all times.



Networking challenges

Information security risks surrounding highly sensitive payment information

Any company with kiosks that store, process, and/or transmit cardholder data must comply with Payment Card Industry Data Security Standards (PCI DSS). Failure to comply can result in fines, lawsuits, and even credit card processing restrictions. If a breach occurs, companies also experience negative publicity that can hinder goodwill with customers, partners, and shareholders.

Connectivity options such as MiFis and USB modems do not comply with PCI guidelines, which include 12 technical and operational components to which companies must adhere.

Unavailable or unaffordable wired connectivity

Kiosks with POS functionality can be a desirable addition to almost any location — whether it's a parking garage in New York City, a hospital lobby in the suburbs, or a service station in a town of 500 people. Because of the widely varying nature of these deployments, organizations are looking to connect their kiosks through all-in-one routers that accommodate both wired and cellular broadband.

Managing widespread IoT with lean IT

Keeping track of cellular signal strength, latency, data usage, and outages among widely deployed kiosks is unscalable when an organization's IT experts are located at headquarters. Internet outages usually require highly expensive corporate travel or third-party truck rolls. As precious time ticks away during an outage, often thousands of dollars of potential transactions are lost.

Benefits of enterprise-grade security and connectivity for IoT systems

Enterprise-grade, IoT-tailored protection of sensitive payment information

Cradlepoint's NetCloud Service for IoT includes robust features and capabilities that organizations utilize as part of their PCI-compliant systems. Cradlepoint's cellular broadband routers include enterprise-grade, comprehensive network security — including a built-in firewall to prevent hacking attempts, as well as the ability to quickly set up VPNs.

For an additional layer of security, Cradlepoint's NetCloud Perimeter feature allows IT teams to set up a private overlay network, which uses Software-Defined Perimeter technologies to completely isolate and hide information over the public Internet. These perimeter-secured overlays can be set up remotely in just a few minutes, and any necessary third-party partners can be added to the network on an invitation-only basis within a private address space.

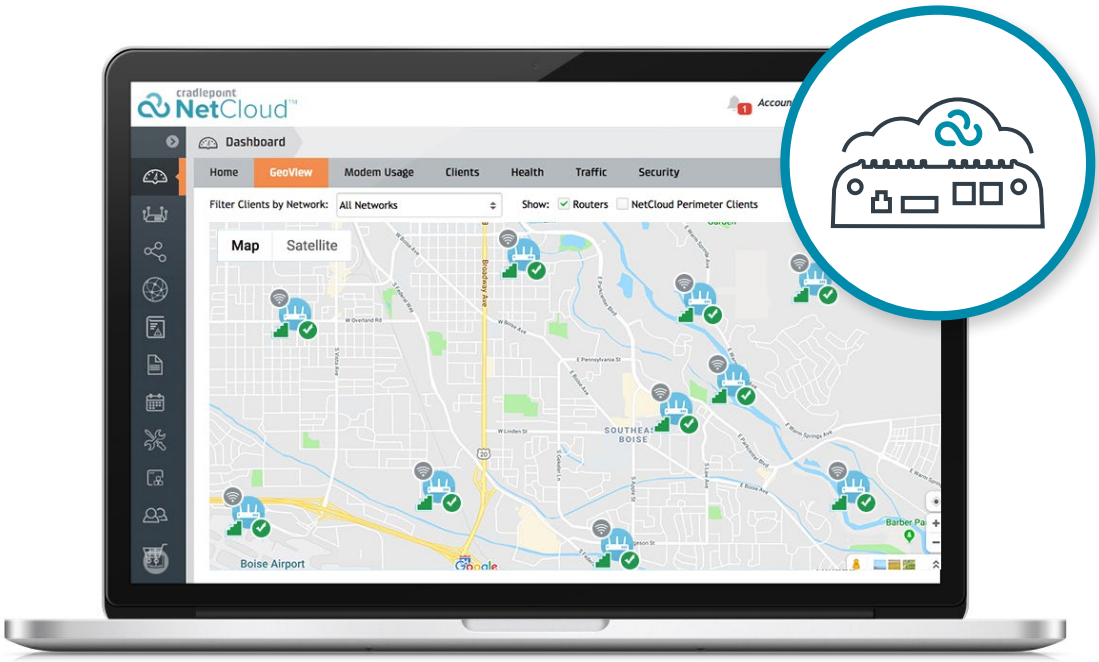
Flexible and cost-effective connectivity for always available payment processing

No matter what type of WAN source is most reliable, cost-effective, and agile in each setting, Cradlepoint's IoT routers with an embedded cellular modem and support for wired broadband keep kiosks' applications and ability to process credit card payments running 24x7. Companies can quickly set up new kiosks with confidence that the network will always maximize their ability to serve customers.

Remote management of cellular connectivity

With Cradlepoint's feature-rich cloud management platform, companies can set up alerts notifying them of WAN outages and signal fluctuations. When an issue arises, the corporate IT team can remotely determine the root cause — and often fix the problem — before ordering an expensive truck roll.

Cradlepoint's NetCloud Service for IoT with wireless edge routers



Explore this solution at **cradlepoint.com/iot-routers**