

Cradlepoint 4G LTE Parallel Networking

CHALLENGE: SECURITY & FLEXIBILITY AT THE NETWORK'S EDGE

The last thing your company's IT executives want to find themselves doing is explaining to an angry public what led to the company compromising customer data. In those situations, there's an immediate hit to the company's reputation, resulting in a loss of brand loyalty, as customers take their business elsewhere. Of course, security breaches are rife with other consequences, such as:

- + Payment Card Industry (PCI) fines
- + Legal costs
- + Loss of proprietary information
- + Lost time and productivity

Enterprises with hundreds or thousands of locations face sizeable, ongoing challenges in maintaining network security and are at high risk of suffering data breaches. As the distributed enterprise's gateway to their corporate WAN, the network's edge is particularly vulnerable to security threats.

Additionally, many enterprises interface with third parties that require access as well. For example, kiosks within stores require



**ENTERPRISES WITH
SMALL DISTRIBUTED
LOCATIONS OR
BRANCH OFFICES
ARE AT THE HIGHEST
RISK OF SUFFERING
DATA BREACHES.**

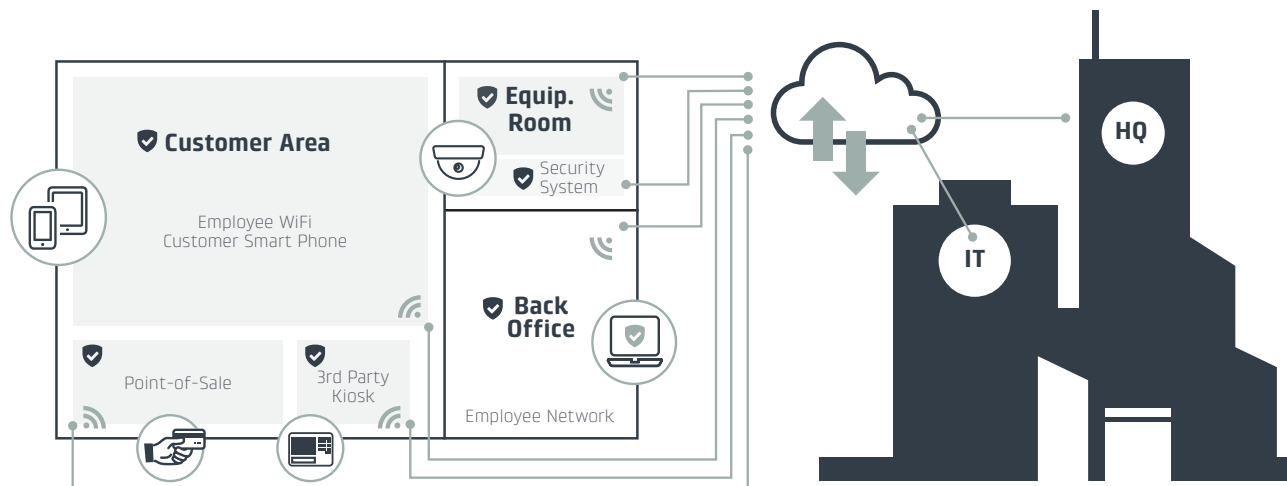


Fig. 1: Parallel Networks Administered by One Source

network access to transmit data, or HVAC vendors need to maintain and control on-site facilities. With multiple parties requiring access and countless risks for security breaches, enterprises spend massive amounts of resources each year developing and updating security protocols.

SOLUTION: CRADLEPOINT PARALLEL NETWORKING SOLUTIONS

While some enterprises implement complex configurations to segment different applications and users on the same network, an increasing number of enterprises are creating “parallel networks” as an elegantly simple alternative. In this scenario, separate applications such as customer WiFi, employee devices, and Point-of-Sale systems are hosted on their own respective networks. Third party vendors, partners, and kiosks must “Bring Your Own Network” (BYON), reducing the company’s overall scope of work in maintaining network security.

CRADLEPOINT'S PARALLEL NETWORKING ADVANTAGES

Save time and reduce scope: Parallel networks reduce the amount of time and expertise needed to segment networks based on application, and limit the effort required for maintaining PCI Compliance on the network used for transmitting cardholder data.

Limit risk: If an employee device or third-party network is compromised, there is no risk that attackers could pivot to other servers and networks, including those that hold sensitive data.

Reduce soft costs: Parallel networks often reduce an enterprise’s soft costs, including the need for complex network configurations that are subject to human error, more complicated PCI Compliance audits, and the general quality of service (QoS) settings for specific applications on the network.

PARALLEL NETWORKING SOLUTIONS

Cradlepoint’s router/firewall devices and cloud-based management software are designed to mitigate security risks and maintain PCI Compliance for distributed enterprises using all types of network architectures. As a cloud-managed solution, Cradlepoint balances the strengths of wired and wireless networks through WAN Diversity™ – the convergence of 4G LTE, Ethernet (DSL, Cable, T1, MetroE), and WiFi as WAN, all delivered through a single networking device.

LEARN MORE: CRADLEPOINT.COM/PARALLEL-NETWORKS