CyberReef

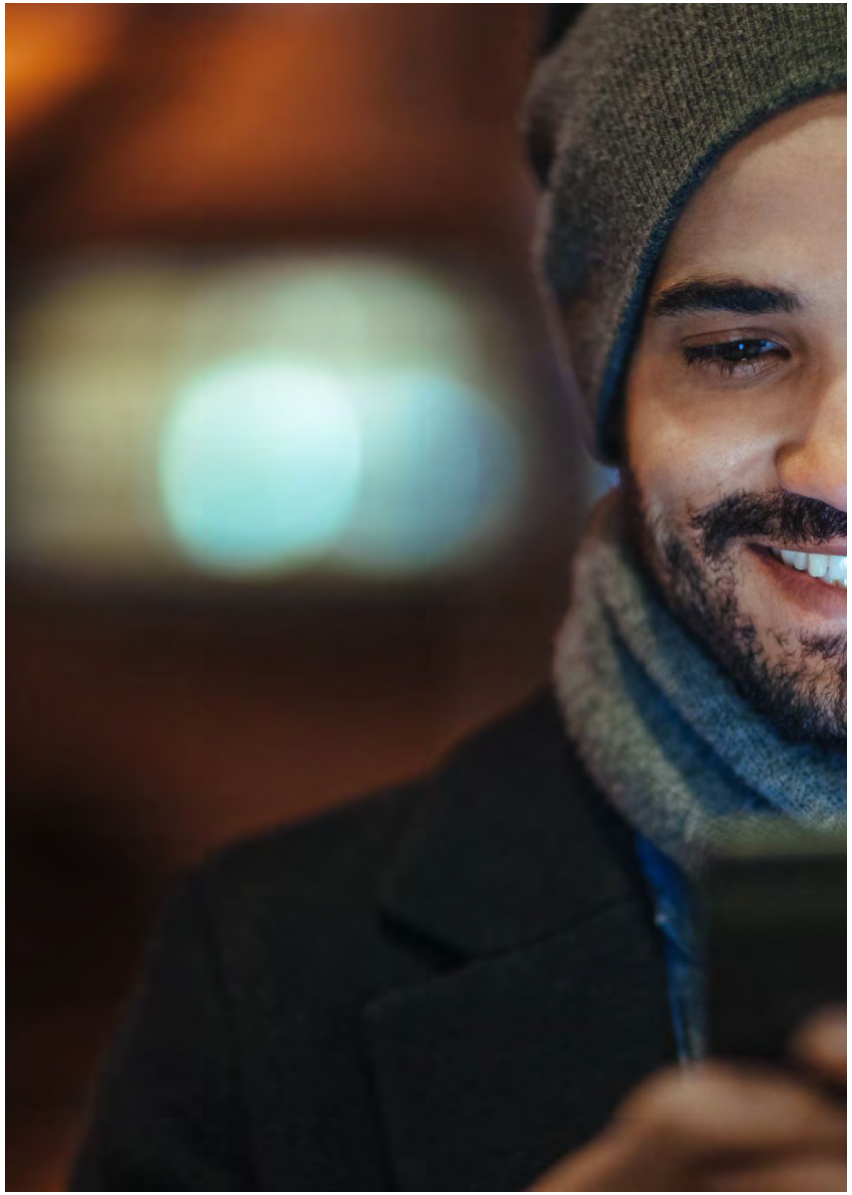
See MobileWall in Action

Discover How Our Mobile Firewall Can Help Your Business

Converge IoT
All things connected

Rural & Underserved Communities

Primary connection for wireless carrier



Problem

A major wireless carrier and a large partner had four **key issues** with primary internet service:

1. Inefficient data usage.
2. Too expensive.
3. No bandwidth control.
4. No remote access.

Solution

By deploying **MobileWall** on a rate plan that we could administer our team was able to:

1. Utilize 6Gbps resource engines for its filtering and throttling technology. We can do this as a single APN or as an aggregate.
2. Half the cost with no drop in service.
3. Application throttling gave them complete bandwidth control.
4. Able to offer remote access with a private network.

Oil & Gas

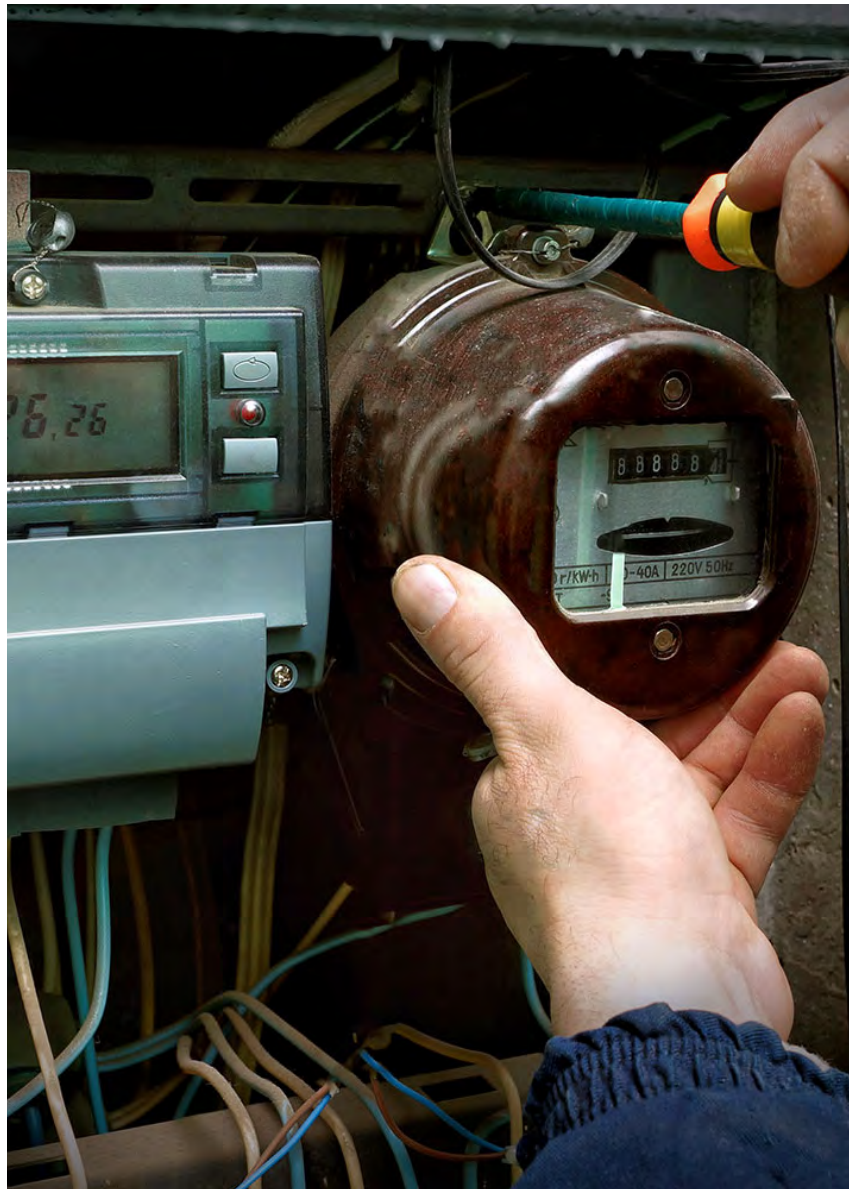
Prevent DDoS Attacks Resulting in Missing Data

Problem

An artificial lift company needed a solution to provide a secure link between remote pump systems for oil production and their operations and a control center to monitor and track critical data from the field. The customer's existing LTE connections were unsecured and continually being hacked by distributed denial of service (DDoS) attacks, leading to data overages and missing data transmissions.

Solution

CyberReef deployed a hosted Private Network and used private static IPs with carrier-agnostic rate plans to keep their IPs from being accessed over the public internet, eliminating the attacks and rogue data consumption. Now, they're able to securely capture and send data over the cellular network to monitor and control centers as well as to cloud-based data centers to share with oil well owners.



Utility

Shield Smart Devices from Malicious Bots

Problem

A public water utility company installed smart meters to collect data from residences. When data usage exceeded expectations, an investigation found cybercriminals attacked the data collection system thousands of times per day. The utility needed intrusion protection.

Solution

The utility worked with CyberReef to set up MobileWall secure access service, which uses a private network backbone that shields devices from malicious bots and hackers. CyberReef used carrier-specific SIM cards on each smart device and added them to a private network using private, static IP addresses. As the utility adds smart meters to their network, those devices are seamlessly added to the existing private cellular network.

Health Care

Secure Mobile Record Keeping

Problem

Nurses for a home health care agency kept written records of patient visits and later entered them into the database. To eliminate insecure, inefficient, and redundant recordkeeping, the agency equipped nurses with tablets, but they needed secure connections and data usage management to prevent costly overages.

Solution

CyberReef built a HIPAA-compliant dedicated APN for the agency, enabling nurses to access and update patient records remotely and securely while blocking unapproved apps like video streaming. The staff saves time, record accuracy is improved, and hospital data costs are kept in check.

Construction

Secure Connections for Temporary Sites

Problem

A large construction site found its wireless surveillance cameras were vulnerable to hacking and its cellular bandwidth limit was exhausted quickly by unapproved uses and rogue devices. The firm needed to improve network security and reduce data usage costs while not limiting the usage of mobile apps and devices required to complete the job.

Solution

CyberReef's MobileWall services provided the construction firm remote connectivity with security, web filtering, and data usage monitoring. By restricting non-business Internet use, the firm improved productivity, secured its surveillance cameras, and reduced mobile data costs by 80 percent.

Fleet Management

Secure Mobile Electronic Logging Devices

Problem

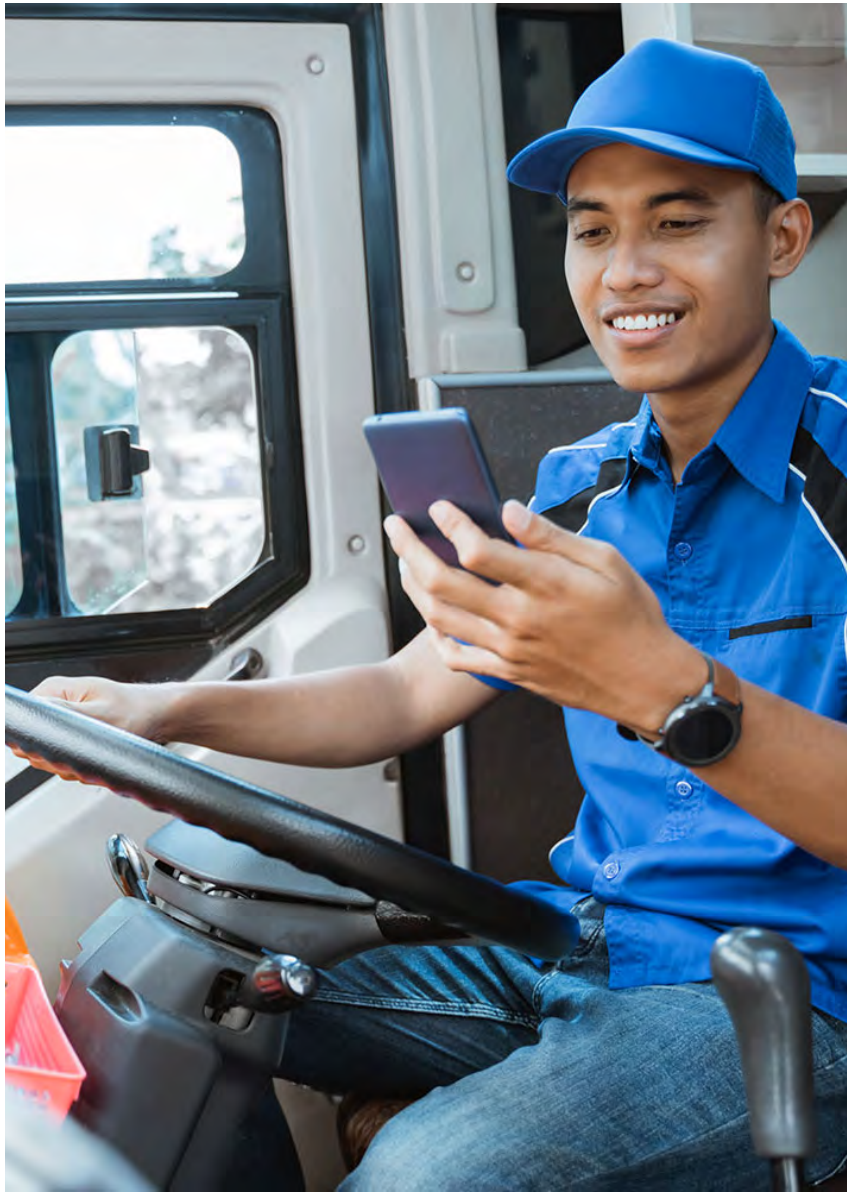
Although a hacker cannot take control of the vehicle through its electronic devices, they can intercept important information that integrates with remote employees and offices. The problem is the vulnerability of data being transferred between the device in the cab, the back office, and the FMCSA's cloud system for transferring the data to roadside officials.

Solution

CyberReef's MobileWall provides a secure connection and offers companies the option to have multi-firewall termination endpoints for data packets. CyberReef can also block all unapproved apps with no additional software, ensuring that the devices are used for the sole purpose of business while helping to keep costs down.

Tour Company

Enabling iCloud for Travelers



Problem

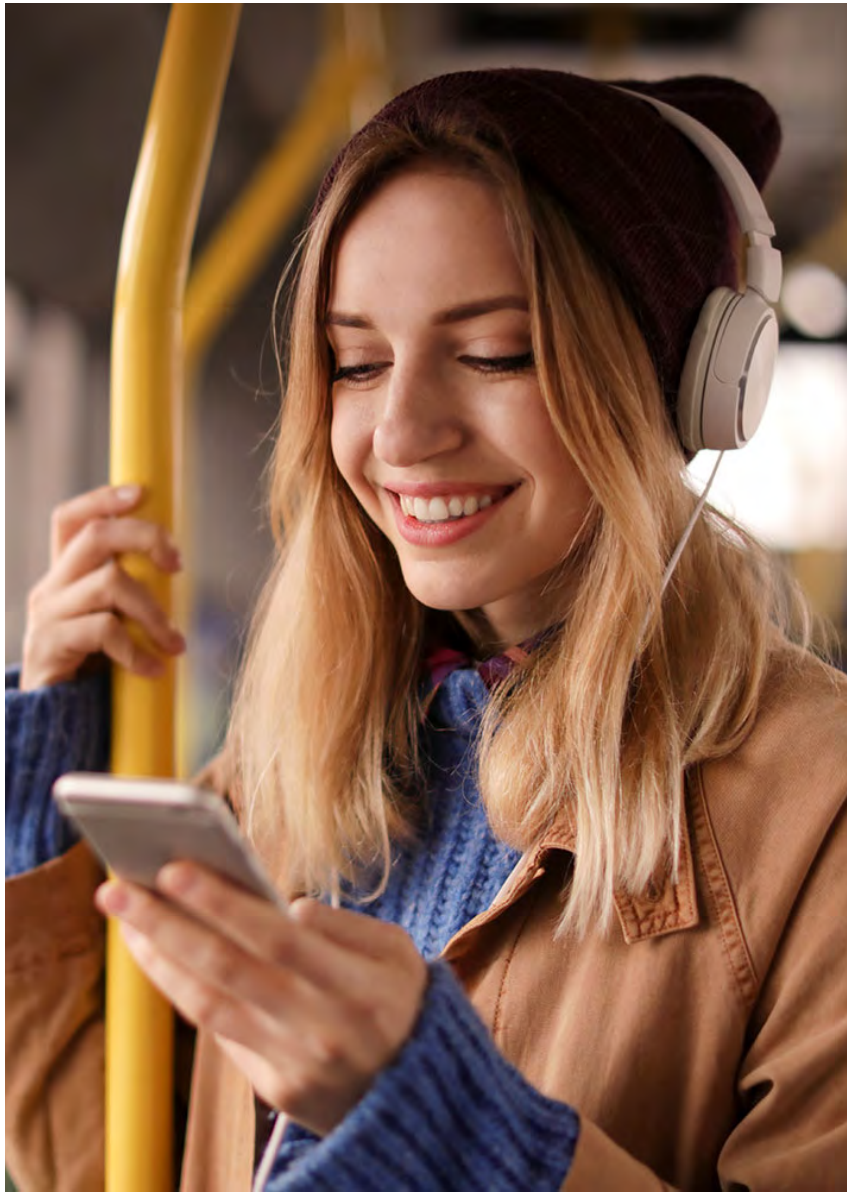
A sight-seeing tour company rented out Mi-Fi devices to tourists promising unlimited data usage for their phones while on the tour. As soon as any Apple devices were connected to the Mi-Fi device, an iCloud backup of all videos, photos, and files would begin, using significant data that the touring company would then be liable to pay for.

Solution

Instead of blocking iCloud altogether, the company worked with CyberReef to block iCloud backup. As a result of this granular level of control, the touring company kept customers happy and cut down on its mobile data usage significantly. The firm no longer needed to purchase an unlimited data plan from their carrier to deliver the service, saving them money and improving their margins.

Transportation

Secure Fare Collection



Problem

A city bus wanted to provide onboard Wi-Fi to its passengers using a broadband wireless router but needed to control the data usage and secure the network to collect fares via prepaid cards.

Solution

The company partnered with CyberReef to enable MobileWall to provide the private networking component alongside the router to quickly and securely validate the passengers' bus passes and allow them to board. Additionally, MobileWall can restrict the usage of high-bandwidth applications like music and video streaming to control data costs and congestion.

Education

Teen-Resistant Content Controls

Problem

A high school allowed students to check out mobile tablets and blocked certain content categories like adult content and streaming video services like Netflix, Hulu, YouTube, etc. They quickly discovered that students could circumvent the content controls by downloading a virtual private network (VPN) to the device, obscuring the DNS, which can also expose them to unmonitored and potentially harmful online content, jeopardizing their safety and well-being.

Solution

Instead of abandoning the mobile device checkout program, the school worked with CyberReef to use MobileWall, which unlike VPNs and DNS redirect solutions, is tied to each device's SIM card. MobileWall also can detect if VPNs are downloaded and block them. Uniquely, policies for access can be assigned to individual schools, grade levels, or individual staff members and can be adjusted to match the curriculum requirements throughout the school year.

Libraries

Affordably Connect Citizens to Community Resources

Problem

To better serve citizens in its community who did not have computing and connectivity at home, a public library received federal funding to supply mobile devices to visitors so they could access job sites, government services, health care, educational resources, etc. Patrons instead were using the machines and bandwidth for streaming video and gaming, running data usage up to 500GB per month exceeding federal funding.

Solution

Rather than restrict what sites users could visit, the library worked with CyberReef to deploy the MobileWall solution to set daily use limits to 1GB per day, per device and then slow the speeds to 1Mbps, so users can still access community resources, but not stream online videos or games in high-definition.

Retail

Affordable, Always-on Point-of-Sale Links

Problem

With 95 percent of transactions being cashless, one restaurant franchise with 2,800 locations needed reliable connections for point-of-sale systems plus a backup failover connection when the primary internet link was down. The customer was concerned about using cellular for failover, fearing high data costs.

Solution

CyberReef enabled the customer to afford the reliable failover necessary. The customer now has always-on connectivity at a low, predictable cost. With MobileWall's secure private network, customer data transmitted at the point of sale remains secure and invisible to hackers.

Retail

Store Kiosk & Kiosk Mode

Problem

With maintaining a steady staff becoming a problem for many businesses, a multi-location retailer was looking for kiosk options for a personalized self-guided checkout experience. The system had to be aesthetically pleasing while still being PCI-compliant and easy to use.

Solution

CyberReef enabled a private network with MobileWall Professional that was able to manage the data on an MDM-protected tablet. The customers were able to login, look up products, and even check out. The retailer was able to continue to stay open during normal business hours with less-than-optimal staffing.

Restaurant - Hospitality

Point of Sale

Problem

With the vast majority (95%) of transactions now cashless, leaving no room for downtime, a major restaurant chain with 2,800 locations relied on dependable connections for its point-of-sale tablets. The tablets they were on were on the public wi-fi network, open to discovery and the transactions were not PCI-compliant.

Solution

CyberReef enabled a cost-effective private network allowing for PCI-compliant transactions and also limited cellular use by locking out any internet traffic that was not related to the POS. The customer now has always-on connectivity at a low, predictable cost. With MobileWall's secure private network, customer data transmitted at the point of sale remains secure and invisible to hackers.

Real Estate

Remote Location Secure Connectivity for Self-Guided Model Home Tours

Problem

Unsecured wireless access presented a security vulnerability for a developer who desired to equip their model home sales office (located in a construction zone) with a data-collecting self-guided tour system. Without a secure wireless connection, the sensitive data collected from potential buyers could be vulnerable to unauthorized access and potential misuse, jeopardizing buyer privacy.

Solution

CyberReef's MobileWall services provided the sales team with remote office secure connectivity, that protected the self-guided tours and kept the buyer's private information secure. The main connectivity was secure and open to all inner office traffic – as long as it was business-related.

Branch & Remote Office

Secure, Business Connectivity for Remote Locations

Problem

A mortgage bank needed secure remote access for both branch offices and at-home workers. After creating an SD-Wan solution for branch offices, it quickly became apparent that this method of creating a secure always-on network for branches as well as remote workers was too costly.

Solution

CyberReef used MobileWall to recreate a corporate-only wireless connection that filtered out all non-business items. In addition, we are creating an always-on function using an MDM and VPN for both the branch and remote offices to save on costs; having CyberReef white glove service without the need to support the costly SD-Wan solution and push out the corporate culture beyond the walls of their offices.