EXPANDING CONNECTIVITY IN REMOTE LOCATIONS

CyberLock®

EXPANDING CONNECTIVITY IN REMOTE LOCATIONS

Enhancing Security Infrastructure with Cellular Routers

In today's increasingly connected world, organizations expect physical security systems to communicate and report in real-time. For remote or infrastructure-limited locations, this can pose a significant challenge. Cellular routers are emerging as a powerful solution for security providers, delivering reliable, secure, and scalable connectivity even in the most isolated environments. This white paper explores the role of cellular routers in strengthening security deployments, reducing operational costs, and enhancing response times in remote security scenarios.

Introduction

Modern security operations rely heavily on continuous connectivity to function effectively. From surveillance cameras and motion detectors to access control systems and alarm monitoring, device performance is typically maximized in installations where equipment can communicate with centralized control hubs or a remote server.

For many companies, connectivity also presents attractive opportunities to reduce operational costs. Networked access control systems offer dynamic scheduling that minimizes downtime. Mobile credentialing makes it easier to leverage temporary contractors, reducing overhead costs. Machine learning and artificial intelligence can continually improve route efficiency and automatically adjust work orders on the fly.

Security providers and system integrators that can expand an organization's digital connection to its remote sites will be able to offer a much broader value proposition. However, traditional wired connectivity is often unavailable or prohibitively expensive in remote or temporary sites—construction zones, remote facilities, critical infrastructure in rural areas, or even pop-up event venues. Many of these locations also have minimal or no security personnel present, escalating the need to access real-time feedback from access control and monitoring devices that are serving as the last line of defense.

Cellular routers present a compelling, cost-effective solution for bridging these connectivity gaps. Many of these devices offer flexible power and connectivity options, streamlining the process for linking up a wide range of edge devices. For critical

infrastructure and other industrial applications where reliability is non-negotiable, several router manufacturers offer rugged, redundant devices that enable security systems to operate reliably in areas where other forms of connectivity fail. Whether it's a telecommunications provider managing contractors at remote towers or a water utility monitoring access to substation gates, cellular routers can provide visibility and real-time control over an organization's remote assets.

Challenges in Remote Security Deployments
Security operations in remote environments face several challenges:

CELLULAR ROUTERS CAN PROVIDE VISIBILITY AND REAL-TIME CONTROL OVER AN ORGANIZATION'S REMOTE ASSETS.

- **Lack of wired infrastructure:** No access to DSL, fiber, or Ethernet.
- **High cost of satellite communications:** Often the only alternative, but costly and slow.
- **Environmental challenges:** Exposure to extreme temperatures, moisture, and vibration.
- **Real-time monitoring requirements:** Lag or connectivity interruptions compromise safety.
- **Delayed emergency response:** Lengthy transit times for emergency personnel mean every second counts.

These constraints demand a flexible, robust solution that is easy to deploy and maintain.

Deploying Cellular Routers in the Security Industry

The versatility of cellular router networks can support a broad range of security infrastructures, including:

1. **Remote Surveillance Systems**
   Deploy IP cameras in isolated areas with cellular backhaul, enabling live streaming, motion-triggered alerts, and cloud storage access.
2. **Physical Security**
   Use cellular routers to provide connectivity to access control system equipment to update credentials, control doors and gates, and upload audit trail information in real time.
3. **Temporary Event Security**
   Set up secure, high-speed connectivity for cameras and access control systems at temporary venues or public gatherings where infrastructure doesn't exist.
4. **Critical Infrastructure Protection**
   Oil rigs, water distribution, wind turbines, and power substations benefit from 24/7 monitoring and control capabilities enabled by cellular modem connectivity.
5. **Mobile Security Units**
   Mounted in patrol vehicles or mobile command centers, the router supports VPN-secured access to HQ systems and remote monitoring tools.

Benefits of Cellular Routers in Remote Sites

Improve visibility and response times with cost-effective network coverage.

- **Rapid Deployment:** No need for trenching or hardwiring; install and activate within hours.
- **Lower Costs:** Leverages existing infrastructure; eliminates need for expensive infrastructure or satellite uplinks.
- **Improved Response:** Enables real-time data and alerts from the field.
- **Scalability:** Easily scale coverage by adding more units.
- **Security & Reliability:** Select models include features like encrypted communication, dual SIM for failover, and centralized management.
- **Global Compatibility:** Deploy LTE CAT 4 Global (G4) routers or LTE CAT 4 Regional routers to tailor coverage to each location.

Cellular Router Capabilities: DGI IX10 Industrial Cellular Router

Security demands reliability. We recommend using an industrial-grade LTE router designed for redundancy. It is important to verify compatibility with your security equipment in a test environment prior to deployment. For CyberLock access control equipment, for example, CyberLock, Inc. has validated the feasibility of using the DIGI IX10 cellular router to support CyberLock communicators at remote sites. Key features provided by the DIGI IX10 router include:

- **LTE[1] Cat 4 North America support with fallback to 3G** for reliability.
- I**ndustrial-grade design** is C1D2 rated with IP30 enclosure.
- **Secure cloud management** to adjust as security needs change.
- **Integrated security protocols** that guard against remote and local intrusion.
- **Dual SIM slots** for failover redundancy.
- **Meets U.S. government FIPS 140-2** cybersecurity standard.

[1] In addition to LTE Cat 4 North America with 3G fallback, Digi IX10 also features configurations for LTE Cat 4 Global with 3G/2G fallback and LTE-Advanced Cat 6 CBRS-only North America.

Case Study: Extending Real-Time Access Control to Remote Sites with CyberLock and the DIGI IX10 Router

Envision a water utility that needs to increase visibility and real-time access control capabilities at a remote site following an unauthorized access attempt by a former contractor. The isolated site presents challenges that traditional security systems struggle to address. Rugged terrain, lengthy perimeter fencing, and exposure to harsh weather conditions require a versatile solution, securing padlocked perimeter gates, a lift barrier for vehicle access, and a new credential reader for real-time management of control room access. Fortunately, CyberLock has the perfect solution.

A COHESIVE ACCESS CONTROL SOLUTION THAT IS ADMINISTERED UNDER A SINGLE, INTUITIVE SOFTWARE PLATFORM

For over 25 years, CyberLock has delivered full-featured access control to the world's most remote locations. Our adaptable solutions are built around a vast range of 400+ durable, electronic lock cylinders that seamlessly retrofit into existing mechanical hardware without network or power cables. In addition to supplying power to the locks upon contact, our industry-leading selection of CyberKey smart keys include networked keys[2] that support near real-time feedback regarding user activity, denied access alerts, schedule changes, expirations, and more.

Three Access Solutions Integrated Under One Powerful Software Platform

With over two decades in the security industry, we learned early on that no two facilities have identical needs. Across the industries we serve, you'll find endless variations in locking hardware, power and network availability, personnel organization, and risk management protocols. Requirements also vary between multiple access points within the same building. Although CyberLock cylinders can be installed virtually anywhere, we recognize that certain locations lend themselves to different technologies. A perimeter gate calls for a different locking solution than the main building entrance, for example. That's why CyberLock's comprehensive system isn't limited to its electronic cylinders, integrating hardwired access control through CyberLock Flex System, as well as a full

[2] CyberKey Blue3 smart keys, for example, sync with the CyberAudit-Web server via a Bluetooth connection to the user's mobile device.
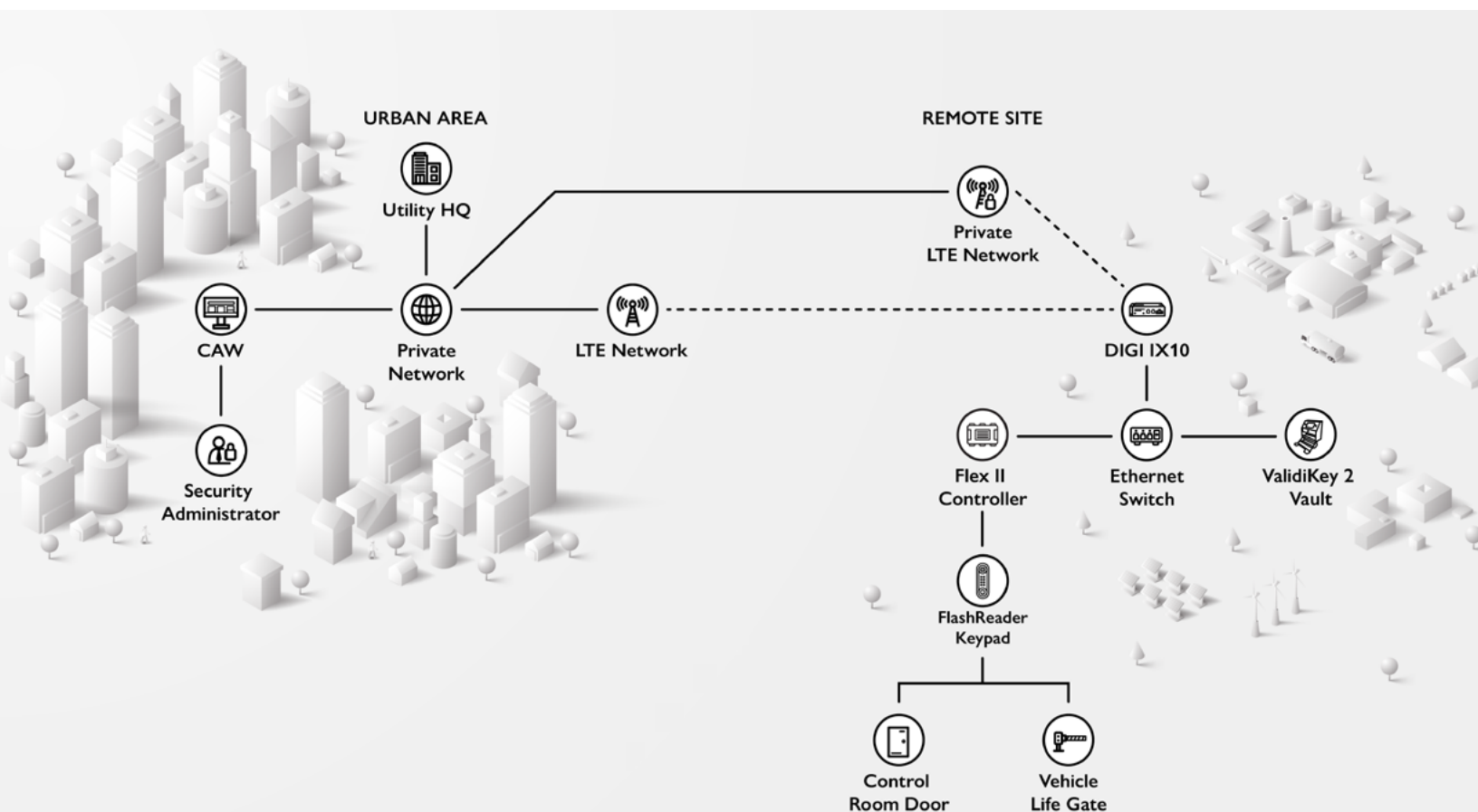
range of keyless locks for mobile credentialing. All three access control solutions come together to create a cohesive access control system that is administered under a single, intuitive software platform, CyberAudit-Web.

Access Control Tailored to Each Access Point
The water utility introduced above can secure its exposed perimeter gates using CyberLock's IP-68 rated padlocks. These weather-resistant electronic locks do not require power or network cables, providing low-maintenance, reliable access control that can withstand harsh, outdoor conditions. Inside the perimeter fencing, however, the water utility may desire even more real-time control over access permissions for both employees and temporary contractors. This level of precision is ideal for networked, hardwired security systems. While power is available at the remote site, the cost of running fiber to provide a wired network connection is not in this utility's budget. Fortunately, the majority of the site is within cellular network coverage. By installing CyberLock Flex System hardwired access control in connection with the DIGI IX10 industrial-grade cellular router, the utility can achieve reliable, real-time access control at a fraction of the cost.

With CyberLock, a facility can deploy a seamless combination of hardwired, key-centric, and keyless access points that are expertly tailored to meet its unique needs. Through CyberAudit-Web's suite of security features, administrators have unparalleled control over access permissions. The real-time control provided by CyberLock Flex System devices is traditionally facilitated using a building's wired network infrastructure. By leveraging the versatility of cellular routers, the utility can extend the precision of hardwired access control far beyond its urban headquarters. With the DIGI IX10 and CyberLock communicators in place, the utility's Director of Security is able to revoke a contractor's access to the remote site in seconds, greatly reducing the risk of unauthorized entry. And with a network connection now available at the remote site, the utility can also install a ValidiKey vault in the control room

BY LEVERAGING THE VERSATILITY OF CELLULAR ROUTERS, THE UTILITY CAN EXTEND THE PRECISION OF HARDWIRED ACCESS CONTROL FAR BEYOND ITS URBAN HEADQUARTERS.

to securely store, charge, and program CyberKey smart keys for accessing the site's perimeter gates.

Despite the many challenges posed by securing the remote site, the utility is able to unlock the full potential of CyberLock's versatile system and remain under budget by utilizing the simple-to-install DIGI IX10 industrial cellular router.

Connect With Purpose

A networked device can present two primary risks to organizations. First, permissive security protocols at a connected device can create a low-resistance gateway that allows attackers to infiltrate other more sensitive areas of the company. Second, a security breach can permit an attacker to actually take command of the networked equipment itself. Access control systems often include devices that are susceptible on both fronts. Cameras and motion sensors, for instance, may serve as low-barrier entry points to the system, whereas unauthorized control of locking devices can inflict serious and immediate harm. When deploying an access control system, it's imperative to understand the risks inherent in connecting your devices.

CELLULAR ROUTERS CAN TRANSFORM HOW THE SECURITY INDUSTRY ADDRESSES REMOTE CONNECTIVITY CHALLENGES.

CyberLock is a pioneer of connected devices in key-centric access control. Indeed, it was CyberLock that launched the industry's first commercially available Bluetooth-enabled smart key and the first Wi-Fi smart key. In each case, the conveniences afforded by these additional communication conduits were carefully weighed against the security risks. CyberLock strives to provide access control solutions that embrace thoughtful connectivity. Connecting a device to your network without a clear benefit is likely to create an overlooked entry point for attackers. Cellular routers can deliver tremendous enhancements for access control and other security products. However, organization's need to be aware that different device manufacturer's will have different security practices, and these devices should be evaluated and configured with the same degree of care as critical IT assets.

Cellular routers can transform how the security industry addresses remote connectivity challenges. Their flexibility, reliability, and cost-effectiveness make them indispensable tools in modern remote security strategies. As security threats evolve, the ability to deploy intelligent infrastructure anywhere becomes a strategic advantage. Whether you are a security provider, system integrator, or facilities manager, cellular routers can serve as a reliable foundation for extending your security footprint.

Contact Us for More Information

CyberLock is the leading supplier of key-centric access control systems, with over 2 million access points secured in 50 countries and growing. We partner with a global network of trained resellers to provide exceptional local support and dedicated customer service. To learn more about how CyberLock products can help your organization protect its future, or if you are interested in becoming a CyberLock reseller, contact our sales team today!