MANAGING DYNAMIC ACCESS CONDITIONS

Securing Critical Infrastructure in a Connected World

CyberLock®

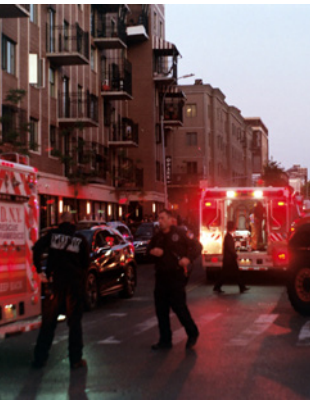
CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com •

MANAGING DYNAMIC ACCESS CONDITIONS

Securing Critical Infrastructure in a Connected World

In Pursuit of Real-Time

The relentless desire to connect electronic devices to one another has fundamentally changed our lives. It has transformed how we consume our news and coffee in the morning. It has revolutionized the way businesses conduct daily operations. It has altered interactions with our neighbors and reimagined the public services that we demand from our communities. And, in many cases, it has redefined our concept of security.



FOR THE ORGANIZATIONS THAT MAINTAIN OUR NATION'S CRITICAL INFRASTRUCTURE SECTORS, THE SECURITY WEAKNESSES INTRODUCED BY POORLY DESIGNED CONNECTIVITY CAN LEAD TO CATASTROPHIC RESULTS.

As we rush to plug our devices into one network or another, it's easy to overlook the potential drawbacks. After all, the benefits conferred by a simple network connection are truly astonishing. However, each new connection introduces uncertainty and complexity, two age-old enemies of security. In our personal capacity, the security risks inherent in universal connectivity are, more often than not, dwarfed by the advantages. The convenience, efficiency, creativity, and endless entertainment afforded by our networked devices distract us from the reality that these very same devices provide a relatively easy conduit to our finances and sensitive personal information. At a community level, however, these risks are amplified exponentially. In pursuing the benefits of real-time alerts, remote access, and cross-platform accessibility, large corporations and government agencies expose much more than the family savings account. It's here that our demand for connection really begins to keep security professionals awake at night. For the organizations that maintain our nation's critical infrastructure sectors, the security weaknesses introduced by poorly designed connectivity can lead to catastrophic results.

Nevertheless, the question for most organizations isn't should we deploy connected devices, it's how quickly can we deploy? In the age of analytics—where every aspect of an organization's operations can be assessed against a slew of metrics—efficiency improvements are the proverbial golden goose. The advantages offered by online devices are too tempting to ignore. Administrators can leverage networked devices to perform

dynamic scheduling that minimizes downtime. The ability to deliver work instructions to a mobile device makes it easier to migrate work to temporary contractors, reducing overhead costs. Machine learning and artificial intelligence can calculate the most efficient route and automatically adjust work orders throughout an employee's shift. Whether you're a publicly traded company seeking to appease shareholders or a power utility responding to growing demand, productivity enhancements are a reliable antidote. With virtually every product segment now offering a "smart version," connected devices can infiltrate even the most mundane aspects of a company's operations. One can even buy a smart, Wi-Fi connected trash can,[1] if so inclined.

PRODUCTIVITY-ENHANCING FEATURES ARE THE VERY SAME FEATURES THAT ALLOW AN ATTACKER TO INFILTRATE THE COMPANY NETWORK

The sheer breadth of operational change can place immense pressure on security and IT departments. The more devices, the more complexity. The quest for the data that both informs and facilitates these efficiency gains often results in a convoluted labyrinth of dependencies between devices, personnel, departments, and databases. Each of these communication links presents an opportunity for a security breach to propagate. The culmination of this organizational rewiring is often an exercise in uncertainty. Each online device presents a gateway inside the organization. After all, the productivity-enhancing features that allow management to update a device from the comfort of their couch, are the very same features that allow an attacker to infiltrate the company network. If an electronic device has an IP address, it can be accessed by anyone with the right resources and motivation. Indeed, businesses and organizations around the globe are impacted daily by these very incidents. According to a recent study by IBM, the average breach costs companies upwards of $4 million USD per incident.[2] For our critical infrastructure sectors, however, security breaches can have devastating consequences that are difficult to quantify. The risks associated with connected devices even extend, perhaps unexpectedly, to security systems themselves. This white paper will demonstrate how organizations operating in the critical infrastructure arena can employ thoughtful connectivity to modernize their access control systems without sacrificing security.

[1] Bruno Smart Can. n.d. Accessed March 10, 2021. *http://brunosmartcan.com/*

[2] IBM. n.d. "Cost of a Data Breach Report 2020." Accessed March 10, 2021. *https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/*

The average breach costs companies upwards of $4 million USD per incident

Protecting our Critical Infrastructure

The U.S. government has long recognized the importance of securing our critical infrastructure—the collection of assets, systems, and networks that are considered "so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, national public health or safety[.]"[3] It doesn't take a vivid imagination to appreciate what's at stake with the integrity of our water supply, for instance. For many of our critical infrastructure sectors, a system malfunction can place thousands of lives at risk. The 190,000 evacuees below California's Oroville Dam[4] can certainly attest to this stark reality. And so it follows that the implications of intentional sabotage or a sophisticated terror attack verge on the realm of the unthinkable.

[3] The definition of critical infrastructure, as we know it today, was established by the USA Patriot Act of 2001, in a section also referred to as the Critical Infrastructures Protection Act of 2001 *(42 U.S.C. § 5195c(e))*

[4] Leslie, Jacques. 2019. "In an Era of Extreme Weather, Concerns Grow Over Dam Safety." Yale School of the Environment. *https://e360.yale.edu/features/in-an-era-of-extreme-weather-concerns-grow-over-dam-safety.*

Fortunately, these threats receive substantial attention at both the public and private levels. Over the previous two decades in particular,[5] government agencies have published a series of regulations and best practices aimed at closing security gaps in our most important infrastructure sites. Without question, these efforts have revolutionized how we monitor and protect vital assets. Visit a critical infrastructure site today and you'll likely encounter identity verification procedures, detailed visitor logs, and a sea of video cameras and access control devices. Most sites are further outfitted with an array of sensors and other monitoring equipment designed to deliver instantaneous alerts regarding system health. The innovations that power this 24/7 monitoring are typically networked devices.

CONNECTED DEVICES DEPLOYED IN NONESSENTIAL DEPARTMENTS CAN CREEP OVER TO A COMPANY'S MORE SENSITIVE OPERATIONS, OFTEN WITHOUT EVALUATING THE SECURITY IMPLICATIONS.

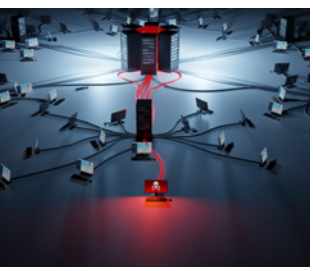
Beyond the regulatory forces, explosive growth and rapid urbanization have effectively required the adoption of networked solutions to keep pace with community needs. Connected devices deployed in nonessential departments can creep over to a company's more sensitive operations, often without evaluating the security implications. Moreover, the COVID-19 Pandemic has further amplified calls for connected solutions at all organizational levels. For certain types of data, like that captured by seismic monitoring equipment at a hydroelectric dam, the near instantaneous access offered by networked devices is non-negotiable. There are many other examples where the benefits of connectivity can mean the difference between a successful evacuation and utter tragedy. At the opposite end of the spectrum are critical infrastructure sectors where connected devices are outright prohibited in certain applications. In most cases, however, weighing the advantages of a network connection against the risk of a security or data breach is less obvious.

[5] Following passage of the USA Patriot Act of 2001, each of the 16 critical infrastructure sectors have been targeted by a wave of regulations, directives, standards, best practices, risk assessments, and security evaluations.

[6] In one of the most publicized examples in recent memory, the retailer Target was hit with a data breach that originated from network credentials stolen from a third-party HVAC vendor.

To Connect, or Not to Connect?

A networked device can present two primary risks to organizations. First, lax security at a device can create a low-resistance gateway that allows a saboteur to infiltrate other more sensitive areas of the company. Anyone who has purchased connected devices for home use has likely encountered the manufacturer warnings that urge buyers to change default passwords and security settings. Despite these risks being well documented, IT departments all too frequently overlook security settings in otherwise innocuous devices like copiers and HVAC equipment. An organization may also provide its network credentials to a service provider or supplier of equipment. In such cases, the third party's failure to adequately protect the credentials can offer a similarly easy path for attackers to wreak havoc.[6] Second, a security breach can allow a digital intruder to actually take command of the networked equipment itself. For something like an air conditioner, this might not present serious danger—a primary reason why security is often overlooked on such devices. A nuclear reactor, on the other hand, carries a substantially higher risk. Certain equipment has the potential to directly sow chaos if operations can be manipulated by an attacker. Although security on these



FAILURE TO ADEQUATELY PROTECT THE CREDENTIALS [OF A NETOWRK] CAN OFFER A SIMILARLY EASY PATH FOR ATTACKERS TO WREAK HAVOC

devices is generally stronger, they still remain susceptible to opportunities created by weak security protocols on other network devices. Access control systems are often found at the intersection between the two risks. Locking devices, in particular, present the final and perhaps only line of defense against a physical breach. In the wrong hands, they have the potential to inflict serious and immediate harm.

When Access Control Becomes Uncontrolled Access

A number of influences have fundamentally altered our workforces over the last decade. The changes have permeated nearly every industry, impacting organizations large and small. Technological advancements, productivity metrics, and job specialization, among other factors, have transformed how companies hire, organize, and deploy personnel.

FOR CRITICAL INFRASTRUCTURE STAKEHOLDERS, A VARIABLE WORKFORCE MAKES IT INCREASINGLY DIFFICULT TO MAINTAIN RIGOROUS SECURITY PRACTICES.

One notable result of this evolution is the emergence of temporary contractors and outside vendors as integral components of an organization's operating plan. This trend has increased pressure to adopt connected devices that make it more convenient to manage a fluctuating, inconsistent labor pool. For critical infrastructure stakeholders, a variable workforce makes it increasingly difficult to maintain rigorous security practices. Several infrastructure sectors impose strict protocols that govern access to secured sites. In the energy sector for example, North American Electric Reliability Corporation (NERC) reliability standards require a physical security plan that ensures each entry into a facility's Physical Security Perimeter involves only authorized individuals and that documentation detailing the event is maintained for at least ninety days.[7] The mechanical access control solutions that have long secured our infrastructure sites are unequipped to address the convergence of regulatory requirements and flexible workforces.

Alongside scheduling and issuing work orders, access control plays an oversized role in the deployment of contractors and outside vendors. The companies maintaining our critical infrastructure require access control solutions that are flexible enough to support variable personnel needs without sacrificing the accountability necessary to comply with demanding regulations. Mechanical locks and keys are too rigid to keep pace. Organizations are already granting access on-demand, to a distributed labor force that changes from one day to the next. Notwithstanding serious concerns over traceability and unauthorized duplication, mechanical keys simply can't be issued quickly enough to meet demand. At the opposite end, networked access control devices undeniably provide the flexibility and convenience necessary to accommodate frequent personnel changes. The value of connected access control devices goes beyond credentialing. Many devices are equipped to deliver a constant stream of data regarding audit trail events, changes in lock status, and tamper alerts. However, for most organizations the real allure of networked access control is the keyless credential. More specifically, organizations are seeking more convenient ways to administer secure area access for visitors, temporary contractors, and outside vendors.

[7] North American Electric Reliability Corporation. 2016. "Cyber Security – Physical Security of BES Cyber Systems, CIP-006-6." Critical Infrastructure Protection (CIP) reliability standards. *https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf.*

THE EASIER IT IS TO GRANT ACCESS TO A CONTRACTOR OR VISITOR, THE EASIER IT BECOMES TO GAIN UNAUTHORIZED ACCESS.

Despite a wave of technological advancements in the security industry, one adage remains stubbornly accurate—to gain convenience, you must sacrifice security. The easier it is to grant access to a contractor or visitor, the easier it becomes to gain unauthorized access. Take keyless entry, for example. By design, users do not need a key to gain access. This means that keys aren't required for intruders, either. Most of us, businesses included, place an undeserving level of trust in our locks, regardless of the apparent level of sophistication or quality. With sufficient resources and determination, any locking device can be opened. This remains true for networked locks, with the added caveat that their accessibility means they can be opened from anywhere in the world using an Internet-connected device. This risk might be acceptable when you need a more convenient way to secure your bike or storage unit, but what about our water supply, airports, or energy grid?

IT IS IMPORTANT FOR ORGANIZATIONS TO SEEK OUT AN ACCESS CONTROL PROVIDER THAT CAREFULLY BALANCES TODAY'S CHALLENGING NEEDS

Security is an ever-evolving concept. A solution that once provided ample protection can become a serious liability as technology evolves. Simply because a device is connected, does not necessarily mean that it is adaptable. Connected devices do not provide a one-size-fits-all solution. Unless we reach a point where security protocols can eliminate the risk of surreptitious remote access, administrators must strongly consider whether they are comfortable using networked locks to secure their critical assets.

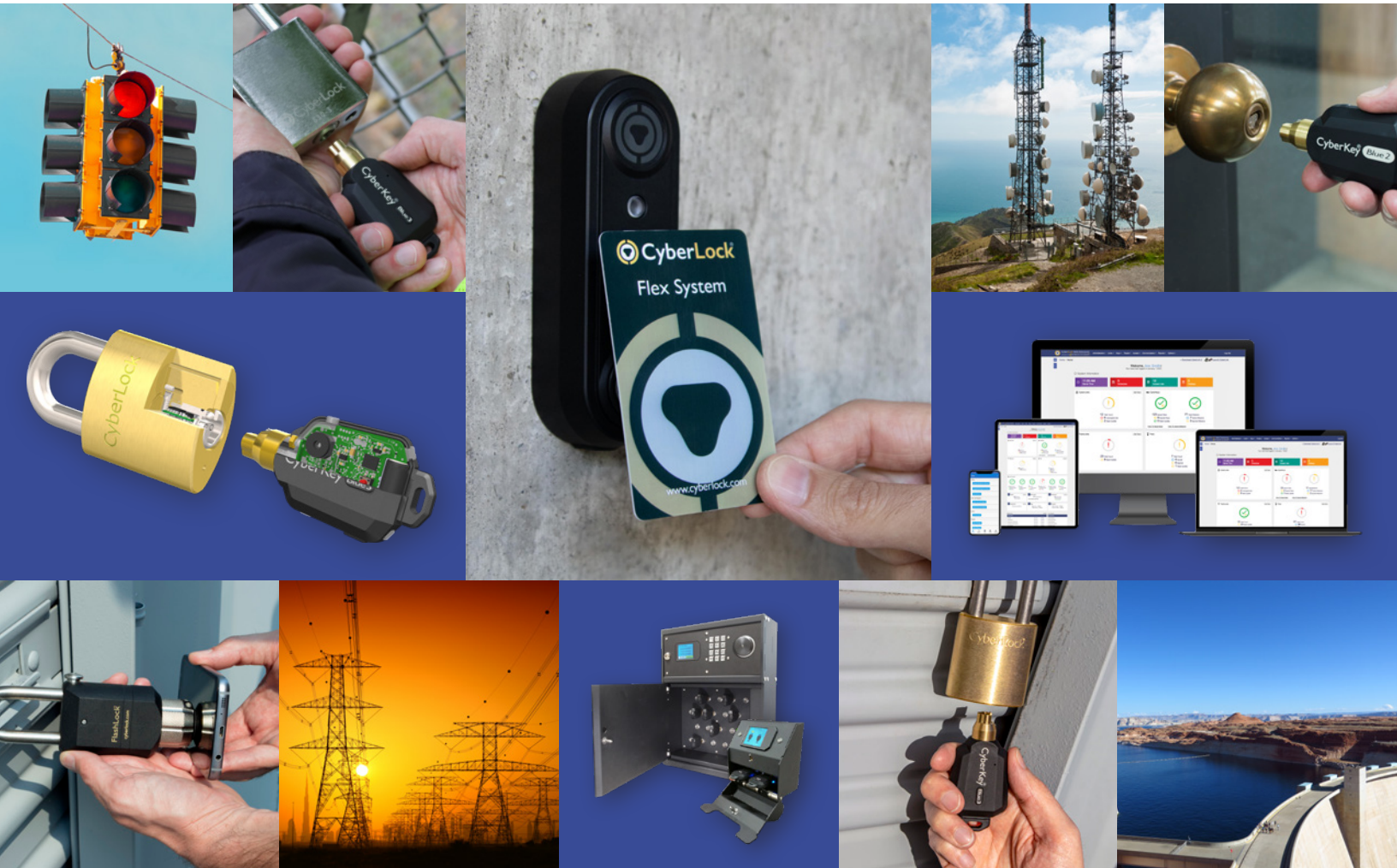
[8] Multiple firms anticipate the global CIP market to exhibit a compound annual growth rate (CAGR) over 6% through at least 2026: for instance, Fortune Business Insights projects the global CIP market to reach USD 154.59 billion by 2027, a compound annual growth rate of 6.2% based on a 2019 estimated market size of USD 96.30 billion, *https://www.fortunebusinessinsights.com/critical-infrastructure-protection-cip-market-103339; while Mordor Intelligence projects a CAGR of 6.49% from 2021–2026, https://www.mordorintelligence.com/industry-reports/global-critical-infrastructure-protection-market-industry.*

Supporting the Next Generation of Critical Infrastructure

Not surprisingly, the critical infrastructure protection (CIP) market continues to exhibit strong growth.[8] The balancing act between security and convenience carries particular importance in critical infrastructure facilities. The emergence of smart cities and persistent threats of devastating cyber attacks are driving rapid investment in CIP solutions. When it comes to access control, critical infrastructure facilities present unique challenges. Administrators are tasked with establishing strict access protocols that must be enforced at a wide variety of entry points, including those at remote, isolated sites. A locking device on a fence, gate, or hatch may serve as the last and only line of defense against unauthorized entry. Alas, it can be cost-prohibitive to deploy sophisticated access control solutions across a multitude of indoor and outdoor locations. Increased reliance on contractors and other on-demand labor adds yet further complexity for facilities that must operate within strict regulatory guidelines. It is important for organizations to seek out an access control provider that carefully balances these considerations in order to support today's challenging personnel needs without opening unnecessary security gaps.

The CyberLock Advantage

For over 20 years, CyberLock has listened closely to the access control needs of our critical industries. We learned that companies need security solutions that can serve a mobile, dynamic workforce. We recognized that productivity and efficiency are not



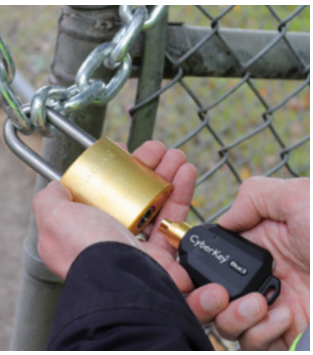
luxuries, but essential considerations in access control. And we embraced the fact that each organization, and in some cases each access point, has its own unique requirements. Most importantly, we know that these needs change rapidly.

At CyberLock, we design access control systems that can be configured for virtually any facility. Our adaptable solutions are built around a vast range of durable, electronic lock cylinders. These 400+ cylinder designs seamlessly retrofit into existing mechanical hardware, providing scheduled access control without the need to install 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[9] that support near real-time feedback regarding user activity, denied access alerts, schedule changes, expirations, and more. With endless hardware configurations and simple installation, CyberLock offers affordable access control to small businesses, churches, and schools. Our scalable systems can easily be expanded and reconfigured as security protocols evolve. The robust CyberAudit-Web management software adeptly manages tens of thousands of access points, bringing accountability to even the largest organizations and critical infrastructure facilities. To truly meet the needs of companies across the entire spectrum, from sole proprietors to multinational corporations, we made versatility an essential design consideration in each product that we produce. By pairing our rugged, install-anywhere cylinders with CyberLock Flex System and FlashLock technology, a facility can deploy a combination of hardwired, key-centric, and keyless access points that are expertly tailored to meet its unique needs. All three technologies come together to create a cohesive access control solution that is administered under a single intuitive software platform.

400+ CYLINDER DESIGNS SEAMLESSLY RETROFIT INTO EXISTING MECHANICAL HARDWARE, PROVIDING SCHEDULED ACCESS CONTROL WITH-OUT THE NEED TO INSTALL NETWORK OR POWER CABLES.

The unparalleled flexibility offered by our three core technologies allows CyberLock to carefully consider how we access and share data across our systems. With organizations that require sophisticated access control capabilities, connecting all of our products would arguably be the easy solution. And yet many of these same customers trust our locks as their last line of defense. Since the first CyberLock was installed in 1999, our electronic cylinders have remained completely isolated from the network. Accountability is an essential element of any access control system. Indeed, there are few scenarios that security departments would consider more troubling than an undetected breach. CyberLock users can rely on the fact that attackers can't surreptitiously access their locking devices from an unknown remote location. Which begs the question, if we are unwilling to compromise when it comes to the security of your locking devices, how does CyberLock support the complex access control needs of today's facilities? Through an innovative system that leverages our powerful family of smart keys to deliver cutting-edge access control features and real-time responsiveness while protecting the devices that matter most: your locks.

[9] The CyberKey Blue3 and CyberKey Flash smart keys sync with the CyberAudit-Web server via a Bluetooth connection to the user's mobile device. The CyberKey Air2 smart key can sync with CyberAudit-Web via an available Wi-Fi network connection.



THE UNPARALLELED FLEXIBILITY OFFERED BY OUR THREE CORE TECHNOLOGIES ALLOWS CYBERLOCK TO CAREFULLY CONSIDER HOW WE ACCESS AND SHARE DATA ACROSS OUR SYSTEMS.

Thoughtful Connectivity

From the origins of CyberLock in the late 1990s, our systems matured alongside mobile technology. In fact, CyberLock is a pioneer of connected devices in key-centric access control. CyberLock launched the first commercially available Bluetooth-enabled smart key—back when companies were still issuing Blackberries to their employees. We followed with the industry's first Wi-Fi smart key, bringing groundbreaking new visibility to the key-centric world. In each case, the conveniences afforded by these additional communication conduits were carefully weighed against the security risks. These early connected keys offered significant improvements in accountability and efficiency. By focusing wireless communication features in the key, we were able to deliver these advantages without exposing our

The FlashReader adds more innovative capabilities and greater control over access points.

locks to the network. CyberLock strives to provide access control solutions that embrace thoughtful connectivity. Every connection comes with increased exposure. For each network link that you add to your access control infrastructure, apply a simple benchmark: the added benefits must significantly outweigh the risks.

A Foundation You Can Trust

CyberLock understands that the stakes are high. The companies that maintain our critical assets need locking devices they can rely on, and versatile access control solutions that don't strain limited operational resources. Our IP68-rated electronic cylinders provide low-maintenance, reliable access control in the harshest environments. These durable locks can be installed anywhere, helping critical infrastructure sectors meet regulatory guidelines on exposed sites ranging from electrical substations to traffic control cabinets to telecom antennas. Since the power is provided by the smart key, CyberLock cylinders do not require battery replacements or downtime for recharging, preserving personnel resources for mission critical tasks. Over the last 20 years our locks have proven they can be trusted. And with cyber attacks now threatening nearly every facet of a company's operations, administrators can count on the fact that CyberLock cylinders are inaccessible to digital intruders. From this secure foundation, CyberLock has designed a thoughtfully connected network of smart keys, communicators, mobile applications, and software that can easily be adapted to each facility's unique requirements. Once deployed, CyberLock systems offer a surplus of features designed specifically for mobile, dynamic workforces. Regardless of your industry, CyberLock can make your employees, contractors, and vendors more efficient, responsive, and reliable.

THESE [CYBERLOCK CYLINDERS] CAN BE INSTALLED ANYWHERE, HELPING CRITICAL INFRASTRUCTURE SECTORS MEET REGULATORY GUIDELINES ON EXPOSED SITES RANGING FROM ELECTRICAL SUBSTATIONS TO TRAFFIC CONTROL CABINETS TO TELECOM ANTENNAS.

Managing a Workforce on the Move

Critical infrastructure sectors around the globe are evolving at a frenetic pace. Technological advancements are driving rapid development of innovative new public services and supporting expansions of physical infrastructure that were previously unfeasible.

Updating a CyberKey's permissions on-the-go with the CybreAudit Link app

Companies serving these sectors have responded by reinventing their workforces to accommodate the faster pace and decentralized nature of this emerging generation of critical infrastructure. However, the organizational resources necessary to support these personnel changes aren't always in place. Existing access control systems may struggle to handle updated procedures for deploying employees, contractors, and vendors. Or, more seriously, facility managers may find that their proposed solutions do not meet exacting regulatory guidelines, exposing the organization to costly penalties and corrective action.

Fortunately, CyberLock offers a wide range of innovative access control products, mobile applications, and software features that are specially designed for a flexible workforce. Whether your organization needs to issue work orders on the fly, deploy remote contractors, or facilitate site access by outside vendors, CyberLock systems help our critical infrastructure customers maintain accountability without sacrificing productivity or security.

The Key to Productivity

CyberLock's versatility is on full display with its industry-leading range of smart keys. Each CyberKey model offers its own unique set of capabilities, allowing CyberLock customers to select the key that best fits how they need to manage access. For organizations that cover a lot of ground—a common occurrence in the Communications, Energy, or Water and Wastewater Systems Sectors—our networked keys can sync with the CyberAudit-Web server from the field, minimizing the need for employees and contractors to return to the office between work orders. Our connected keys, including the award-winning CyberKey Blue 3 and CyberKey Air 2, support a number of features that enhance productivity and accountability for workers that are always on the move.

The ValidiKey 20 securely stores, charges up to twenty CyberKey smart keys, and syncs with CyberAudit-Web and the user's access permissions.

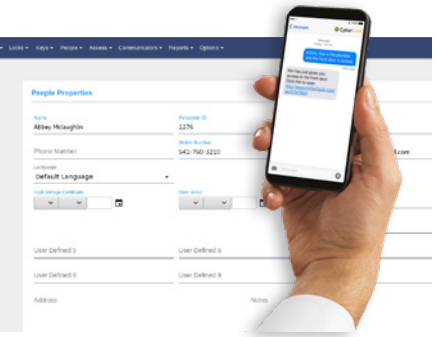
When the power is in the key, quite literally, your workforce needs convenient charging options. A micro-USB port[10] allows your team to charge their smart keys from virtually anywhere, even their vehicle. For organizations that want additional accountability, keys can be securely stored, charged, and programmed from a ValidiKey vault, ensuring your crew is always prepared with a fully-charged, up-to-date smart key. Other customers prefer the flexibility offered by the replaceable batteries of the CyberKey X.

CyberKey Blue 3 delivers an exceptionally powerful tool for controlling access to isolated sites and sprawling facilities. Blue 3 enhances system security by supporting temporary access and delayed activation, extending precise access control features to the most isolated locations. With CyberKey Blue 3, users can receive access permissions when in cellular range, cache the permissions via the easy-to-use CyberAudit Link app, and later activate their key outside of cellular range. This makes the CyberKey Blue 3 an ideal smart key for critical infrastructure security at remote locations.

[10] USB charging capability is available on select CyberKey models.

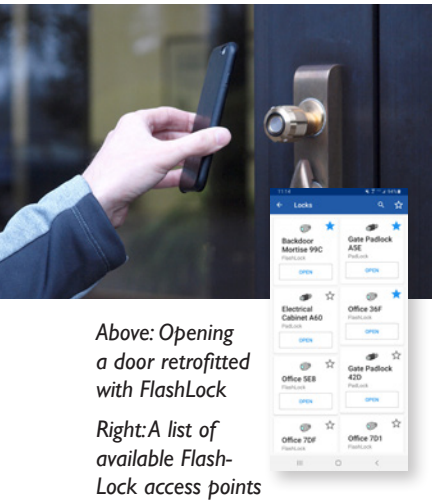
Access in a Flash

When organizations need credentials that are truly mobile, they go keyless with our award-winning FlashLock technology. Our patented mobile credential system provides fast, hassle-free access in seconds. Other access control systems make granting permissions to remote contractors or outside vendors far more complicated than it needs to be. For the companies that support our critical infrastructure sectors, time is too precious to waste. The last thing a facility manager wants to worry about is trouble-shooting a contractor's user account registration or waiting for a vendor's IT department to approve a smartphone app for installation. With FlashLock, granting access is as easy as sending a text or email. Better yet, this functionality is integrated right into CyberAudit-Web, allowing administrators to send keyless credentials with a few clicks of their mouse.



Sending/receiving a FlashLock access link via text message

For users in the field, the process is just as simple. Using the link sent to their text messages or email inbox, workers can access personalized web-based access credentials

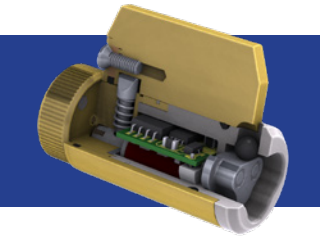


Above: Opening a door retrofitted with FlashLock

Right: A list of available Flash-Lock access points

directly from their smartphone's web browser. With a single link, administrators can grant scheduled access to one or more doors, padlocks, and keyboxes. Increase control over keyless access points by setting narrow time slots during which access is authorized.

Using our serial optical communication technology, access credentials are delivered from the user's phone screen directly to the lock. Without a user account or dedicated smartphone app required, access can be granted in seconds. For users that are unlikely to access an organization's locks on a frequent basis (e.g. A repair technician from an outside vendor), FlashLock access points significantly reduce the administrative overhead involved with issuing temporary access credentials. The recipient's access activity is tied to their mobile number, providing accountability even for one-time users. As with all CyberLock products, administrators can generate time-stamped audit reports detailing who entered their access points. For more frequent FlashLock users and administrators, CyberLock offers mobile applications that deliver additional functionality. With multiple ways to issue FlashLock credentials, companies can tailor the system to their own access protocols.



WITHOUT AN IP ADDRESS, YOUR LOCKS REMAIN PROTECTED FROM HARD-TO-TRACE CYBER ATTACKS

While our keyless credentials deliver exceptional convenience for temporary workers, contractors, and outside vendors, our priority will always remain the security of your locking devices. Like CyberLock cylinders, FlashLock access points are not connected to the network. Without an IP address, your locks remain protected from hard-to-trace cyber attacks. People, however, are not the only threat to an access control system. Our customers operate in some of the planet's most demanding industries. They know that keyless access points aren't always needed at convenient, sheltered locations. In designing FlashLock to support these customers, we applied the same expertise that has kept our CyberLock cylinders in the field for over 20 years. Our FlashLock padlock is IP-68 rated, bringing the convenience of our efficient mobile credentials to harsh environments and exposed outdoor locations. Whether you need key-centric or keyless functionality, we supply electronic locks that can be trusted wherever they are deployed.

CyberLock features dynamic key-centric security and communication

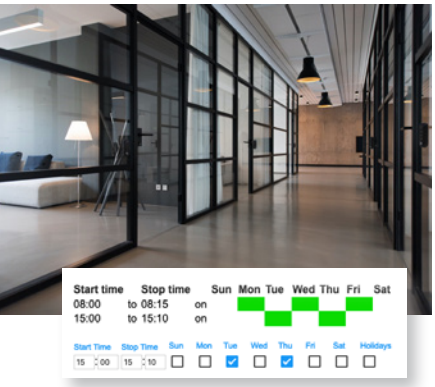
Hardwired for the Future

Although CyberLock cylinders can be installed virtually anywhere, we recognize that certain locations lend themselves best to hardwired solutions, like wall-mounted readers. CyberLock Flex System allows our CyberLock customers to retain the benefits of hardwired access control on high-traffic doors, turnstiles, and other entry points.

Using the FlashReader to access a hardwired door controlled by CyberLock Flex System

Our commitment to versatility doesn't stop with our key-centric and keyless solutions, CyberLock Flex System supports an array of features to help accommodate unpredictable personnel needs. For instance, the latest hardware innovation in our Flex System family is the FlashReader, a multi-credential, wall-mounted reader for hardwired access points. To gain entry to an area controlled by a FlashReader, users can present traditional RFID cards or use our Flash technology for a convenient keyless credential. Future releases of the FlashReader will support at least two additional credentials, yet another keyless option using Bluetooth Low Energy (BLE) and a PIN credential entered via an integrated keypad. With the potential to support up to four different credentials, FlashReader wall-mounted readers give your organization the ultimate flexibility to adjust access control protocols as your needs evolve.

When it comes to our critical infrastructure sectors, personnel deployment must be accurate and efficient. We've already discussed how CyberLock provides a variety of ways to swiftly grant access to its vast range of key-centric cylinders and keyless access points. However, most companies also need to deploy workers to indoor locations secured by traditional card readers and other hardwired devices. While RFID cards are inexpensive and readily available, the resources required to activate and issue cards to temporary and one-time users can prove burdensome. Moreover, the COVID-19 pandemic has driven demand for contactless solutions that minimize user contact. In addition to the multi-credential versatility of the FlashReader, CyberLock has extended the convenience of its web-based credentials to its hardwired systems.



CyberLock Flex System offers precise control over offices and other hardwired access points

Custom short-term access schedule

Regardless of facility size, contractors, vendors, and other visitors will inevitably need access to hardwired entry points. Often installed in well-monitored areas, with multiple layers of protection, hardwired doors can also support enhanced convenience without significantly impacting security. With Remote Door Access, a new feature introduced in CyberAudit-Web 9.4, issuing credentials to hardwired doors has never been easier. Other access control systems require significant resources to support their keyless credentials, whether it's registering user accounts, obtaining IT approval for installing new applications on company-owned smartphones, or maintaining compatibility with third-party devices. With CyberLock Flex System, granting access to hardwired doors is as easy as sending a text or email. Similar to our FlashLock keyless credentials, Remote Door Access facilitates scheduled access without the need to register a user account or download a dedicated mobile application. Instead, users need only a web browser and Internet connection.

From the CyberAudit-Web interface, administrators define scheduled access to one or more hardwired doors. For large facilities, CyberAudit-Web's batch scheduling capabilities simplify the process of granting access to groups of doors or groups of users. Once permissions are set, Remote Door Access delivers a hyperlink to the user via text message or email. There's no need to coordinate delivery of a physical RFID card or provide detailed instructions on how to download and configure a mobile app. By accessing the text message or email link, users can open hardwired doors directly from a web browser on their smartphone.

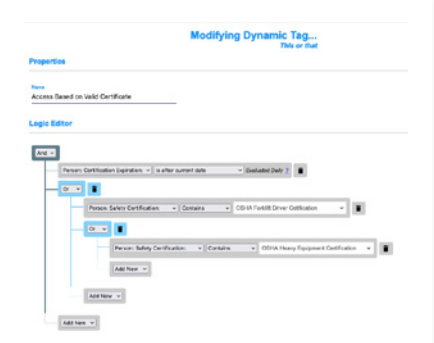
BY ACCESSING THE TEXT MESSAGE OR EMAIL LINK, USERS CAN OPEN HARDWIRED DOORS DIRECTLY FROM A WEB BROWSER ON THEIR SMARTPHONE.

In most hardwired systems, credentials are presented to a card reader near the door. With Remote Door Access, doors are triggered directly from the user's web browser by sending a request to the server via an available cellular or Wi-Fi network. For instance, when

Administrators can send Remote Door Access with a few easy clicks in the CyberAudit-Web interface

a contractor arrives at a door she can click the link from her text messages to open the Remote Door Access web interface on her smartphone. Provided the contractor has arrived during her authorized schedule, she can open the door by selecting it from the list of available doors. The request is sent to the server, which logs a detailed audit trail of the event and transmits a signal to the door to trigger the electric strike.

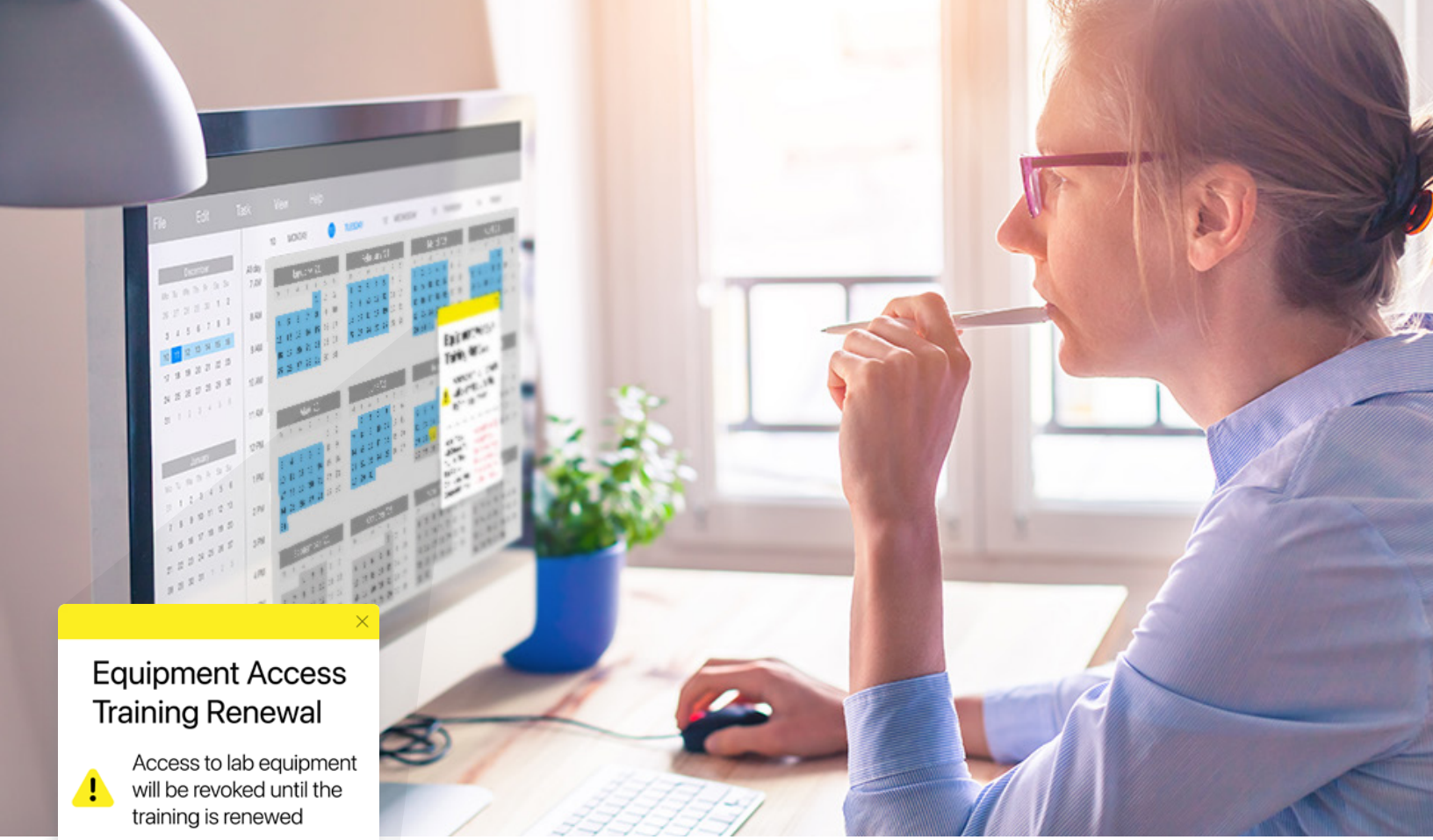
The entire process is completed in just seconds. Moreover, the contractor didn't need to worry about whether her outdated smartphone would successfully pair with the door reader. Once the contractor's schedule has expired, the doors are no longer available in the Remote Door Access interface, preventing access outside of the scheduled time window. For organizations concerned with health and safety protocols, Remote Door Access gives administrators a convenient, contactless solution for issuing hardwired door credentials. The versatility offered by this feature is also ideal for facilities that have personnel working remotely. Even in the event an employee or contractor forgets their phone at home, management can use Remote Door Access to open doors on their behalf by sending request-to-open commands from their own web-enabled device.



Create custom tags that support your facility's specific risk management protocols

Permissions That Update Themselves

Companies that support our critical infrastructure have developed robust risk management strategies. It is imperative that an organization's access control system can accommodate its risk management protocols without severely impacting security or productivity. In some industries, for example, workers must possess certifications that demonstrate they are trained to operate or service certain equipment. Generally, it is left to management to manually verify that an employee has maintained the necessary certifications. Some larger organizations may have human resources systems that flag employees with expired certifications, but without an access control system that can respond to these changes the employee may still have access to the high-risk areas or equipment. CyberLock recognizes that these risk management protocols are too important to leave to chance. The Dynamic Tags Software Enhancement Module (SEM) for CyberAudit-Web gives organizations an access control system that automatically adapts to changes in personnel and environment.



Dynamic Tags can automatically revoke access to protect your most important assets

With Dynamic Tags enabled, administrators can create one or more 'tags' that define additional criteria for granting access. CyberAudit-Web evaluates the tags periodically, automatically adjusting access permissions based on whether or not tag criteria is satisfied. Because the tags are user-defined, the criteria can be customized to support a broad range of risk management protocols. When a user syncs his or her CyberKey smart key with the server, the key is updated with the latest permissions. By setting keys to expire frequently (e.g. daily), a facility can ensure that a user's access permissions automatically reinforce the current risk management protocols.

Let's say, for example, that a day-shift employee is required to complete annual training on certain equipment that poses a serious risk to operators. In addition to scheduled permissions that authorize access to facility locks between 8am–5pm, the employee's permissions are also subject to an equipment training tag. The tag can be applied only to the specific locks that secure the dangerous equipment, allowing the employee to access other areas of the facility even if the periodic training is not completed. A CyberLock administrator configures the tag to use a training expiration date as input. Training expiration data can be entered manually, or retrieved automatically from a database. CyberAudit-Web evaluates the tag daily to determine whether the employee's training has expired. If the employee fails to complete his training within the required time frame, CyberAudit-Web will automatically revoke the employee's access permissions on the expiration date. If the employee later completes the training, CyberAudit-Web's will recognize the new expiration date when it performs its next tag evaluation and permissions to access the dangerous equipment will be restored.

IF [AN] EMPLOYEE FAILS TO COMPLETE HIS TRAINING WITHIN THE REQUIRED TIME FRAME, CYBERAUDIT-WEB WILL AUTOMATICALLY REVOKE THE EMPLOYEE'S ACCESS PERMISSIONS ON THE EXPIRATION DATE.

This automated process minimizes the risk that permissions are not promptly updated after a change in user qualifications. For medium to large-scale facilities, the Dynamic Tags SEM helps administrators more efficiently manage access for large numbers of key

holders. By reevaluating access rights on a frequent basis, Dynamic Tags can automatically grant or revoke access without requiring manual input from a system administrator or security manager. Improve security by ensuring that a user's access is revoked if safety or training certifications have expired. Boost productivity by seamlessly granting access rights when key holders satisfy the necessary prerequisites. Dynamic Tags delivers a tailor-made access control solution by giving administrators the power to define access criteria that is most important for mitigating risks in their particular facility.

Three Technologies Integrated Under One Powerful Software Platform

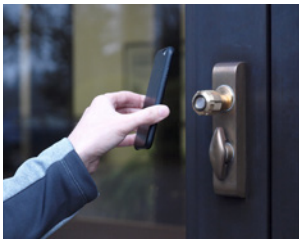
With over two decades in the security industry, we've tackled a lengthy list of access control challenges. We've learned that no two facilities have identical needs. Across the 16 different critical infrastructure sectors, for instance, you'll find endless variations in locking hardware, power and network availability, personnel organization, and risk management protocols. Requirements also vary between multiple access points within the same building. A perimeter gate calls for a different locking solution than the main building entrance. Yet for some critical infrastructure sectors, the rarely used perimeter gate and high-traffic main entrance are both subject to the same stringent regulatory requirements governing authorized access.[11] It is vital that a company's access control infrastructure is equipped to handle the unique challenges presented at each of its many entry points.

In CyberAudit-Web, customers can easily manage access to key-centric CyberLock cylinders, keyless FlashLock access points, and hardwired CyberLock Flex System doors, all from the same intuitive interface. CyberLock is the only solution that offers administrators cohesive control over all three access control technologies. Even after investing significant resources in integration, other systems may still require management to switch back and forth between consoles or logins, duplicate permission management, or issue multiple credentials to employees and contractors. With CyberLock, a single CyberKey Flash smart key can open CyberLock cylinders, transmit IR credentials to unlock FlashLock devices, and emulate an RFID credential to access hardwired doors. Regardless of your industry, CyberLock has the right solution for every access point in your organization.

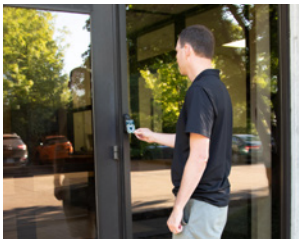
[11] In the Transportation sector, for example, 49 CFR § 1542 compels airport operators to prevent and detect unauthorized entry into their air operations area (AOA). Typically encompassing aircraft movement and parking areas, an airport's AOA can be a vast area that extends well beyond terminal buildings.

A multi-state power utility company uses Cyberlock for its dynamic security needs. CyberLock's three unique technologies help support their vast mobile workforce. CyberLock's security solutions provide access control for entry points that span any physical environment.

Key-centric

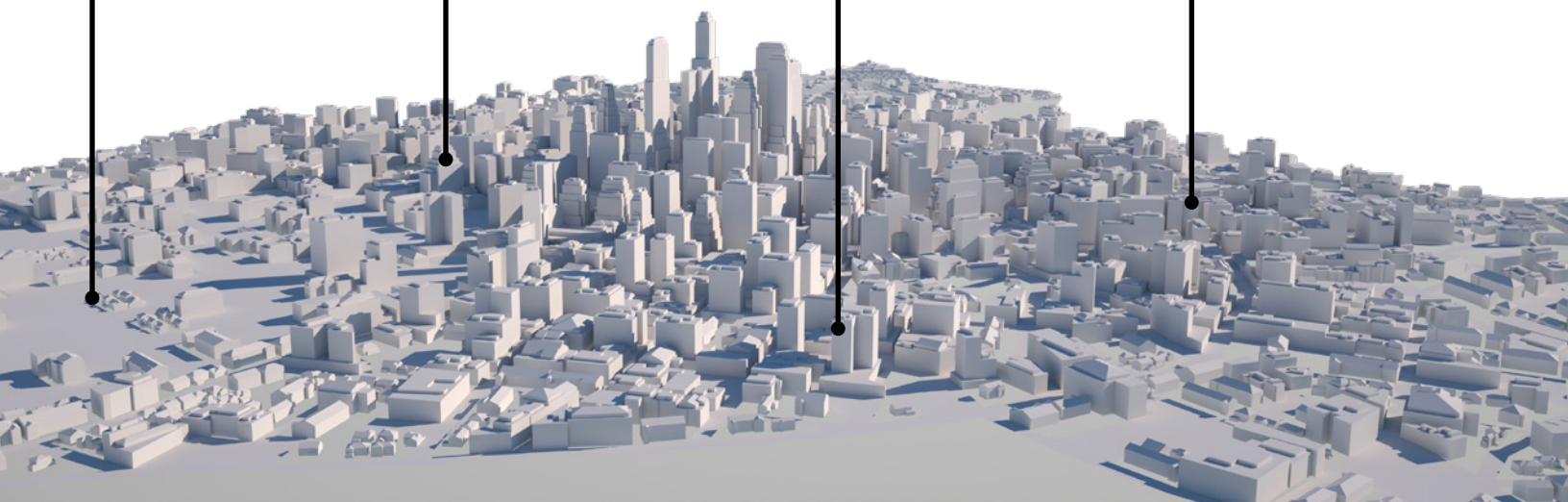


Flash Technology



Flex system

Mobile CyberKey update



Conclusion

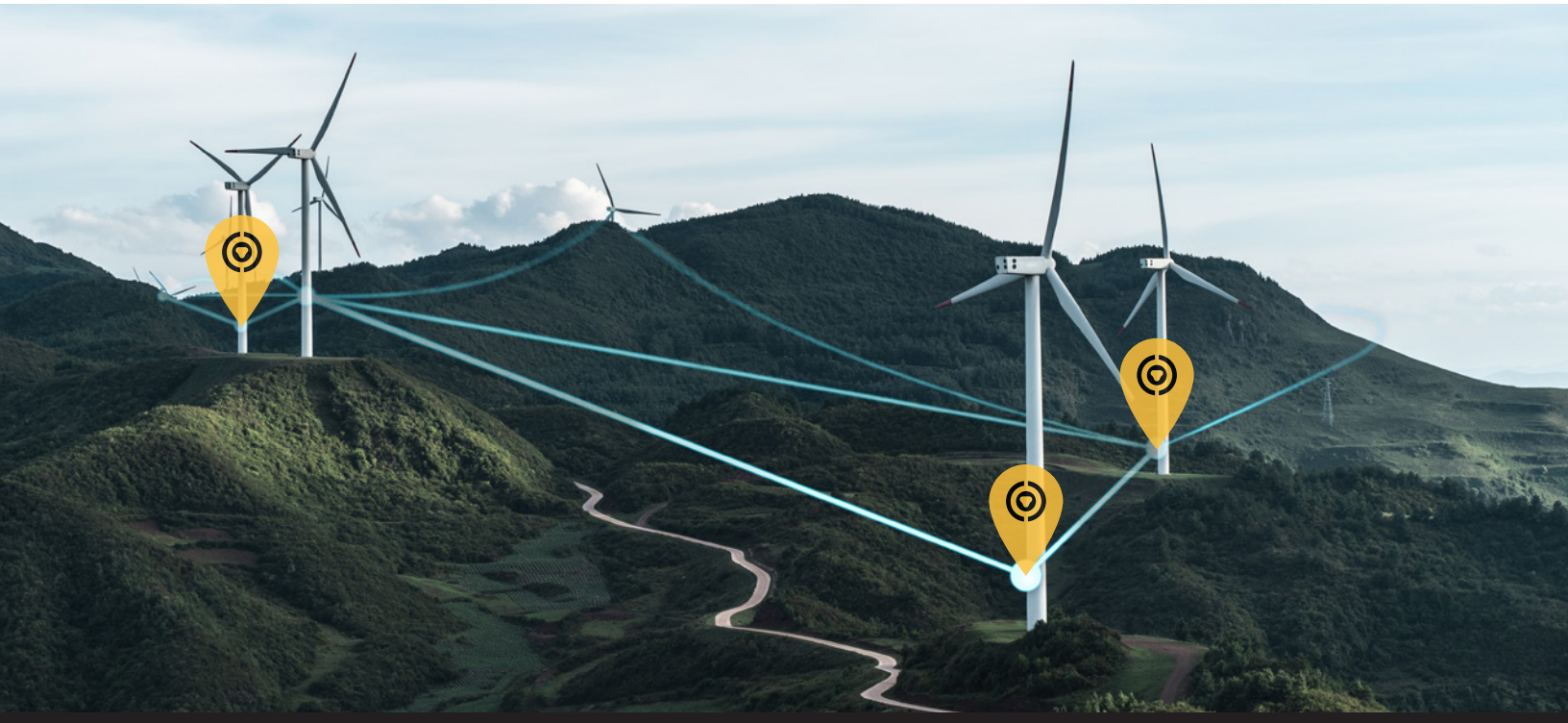
Access control plays an important role in maintaining critical infrastructure resources. The health and safety of our communities depend on the efficacy of security and risk management protocols implemented by various infrastructure stakeholders. Ultimately, organizations need access control devices they can trust. With little margin for error, the balance between security and convenience is tilted decisively toward security. The high stakes make it difficult for companies to accommodate emerging workforce trends. The next generation of critical infrastructure operators should be prepared to invest in an access control solution that can support a distributed, fluid labor force without sacrificing security.

For over two decades, CyberLock access control devices have been trusted to protect critical assets around the globe. In fact, some of the first electronic cylinders we deployed are still in operation today. While these durable locks haven't moved much over the last 20 years, the world around them has endured a whirlwind of change. We understand that our access control solutions must evolve alongside the industries we serve. Adaptability is a primary design consideration in all CyberLock access control products. From small, rural water utilities to massive, multi-national telecommunication providers, CyberLock can help your workforce carry out its mission with confidence, efficiency, and accountability.

An access control system is too important to be a short-term investment. We take pride in the fact that every CyberLock product is designed, manufactured, and assembled entirely in the United States. Our commitment to quality permeates every aspect of product development to ensure that CyberLock systems are built to secure our communities for the next 20 years and beyond.

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!

* The content provided in this white paper is current as of May 2021. Features of CyberLock access control products and CyberAudit-Web management software may change in the future as we continually strive to find the perfect balance of convenience and security for our customers.



CyberLock®

CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com •