BLUEWARRIOR

Take Charge of Your Security and Compliance with BlueKey™ Encrypted Locks & Automated Software



Patent Pending

The BlueWARRIOR-Cloud Is Secure: Cyber-Blue - developed by BlueWARRIOR for BlueKey™

You hear a lot about cloud security lapses and high-profile breaches in the news. Industry reports and analysts exhaustively cover sensational cases publicly. But if you dig deeper into the details of these breaches, you'd discover that most of these vulnerabilities could have been avoided if the cloud environment was configured according to cloud security and compliance best practices. The IV Cloud is secure.

Introducing - Cyber-Blue - Hosted by IV for BlueWARRIOR's Bluetooth Locks. Each customer subscription has its own secure cabinet. **Cyber-Blue** automatically records, tabulates and analyzes lock data

Cyber-Blue features include:

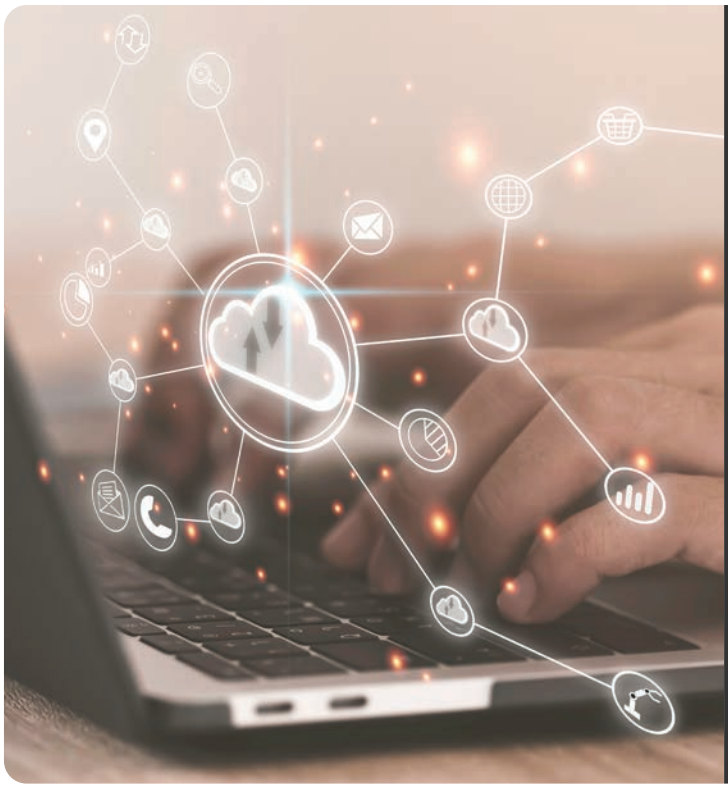
- Low Cost - Easy to Operate
- Secure Cloud Application
- Cyber-Secure
- Built in Data Analysis
- Complete & Full Audit Trail of All Locks
- Accurate Data & Time stamp for every transaction
- Program Keys to control who has access to assets
- **Program key for when & what time period for access**
- **Data Analytics provide a visual audit of suspicious activity.**
- **Create and Change Access Rights & Schedules**
- **Program a Key to expire at a specific time & no longer operate**
- **Pre-configured Access Profiles**
- **Infinitely Virtual Cloud Security**
- **BlueKey™ Family of Products**
- **Meets NIST Security Guidelines**

Access Control - Fully Automated and In the Cloud - and Accessible by Mobile Phone

Today - Cloud Services have become part and parcel of our daily activities. This cloud subscription service is flexible, affordable and most importantly - SECURE. Today you can manage your locks and and infrastructure assets. Imagine - a Full Audit Trail for each and every lock. No exceptions. No tampering. No duplicated keys. No Number 2 key. No picked locks. All data and transactions are encrypted. No duplication of keys. No contaminated or altered records. Full time and date stamp for each and every lock transaction. BlueWARRIOR has partnered with IV to bring you low cost data security and automation. We provide a secure cloud application - you have an easy to use application. Cyber-Blue provides Security, Accountability and Compliance (NIST) for every lock transaction.



> Through 2023, 99% of cloud security failures will be the customer's fault.
>
> – Gartner, CSO Online 2021.[i]



> More than half (58%) of survey respondents are concerned about security .
>
> – CSA Survey, 2021.[ii]

Role of Encrypted Bluetooth Locks in Supporting Critical Infrastructure Assets

Utilities need to support the established resiliency strategies of: Assessment, Prevention, Detection and Recovery. This strategy not only includes network perimeter hardening but also encompasses Cyber-security, communications and equipment redundancy. The System Operations & Management Center needs to be hardened, protecting critical substation assets, and recovery from all events.

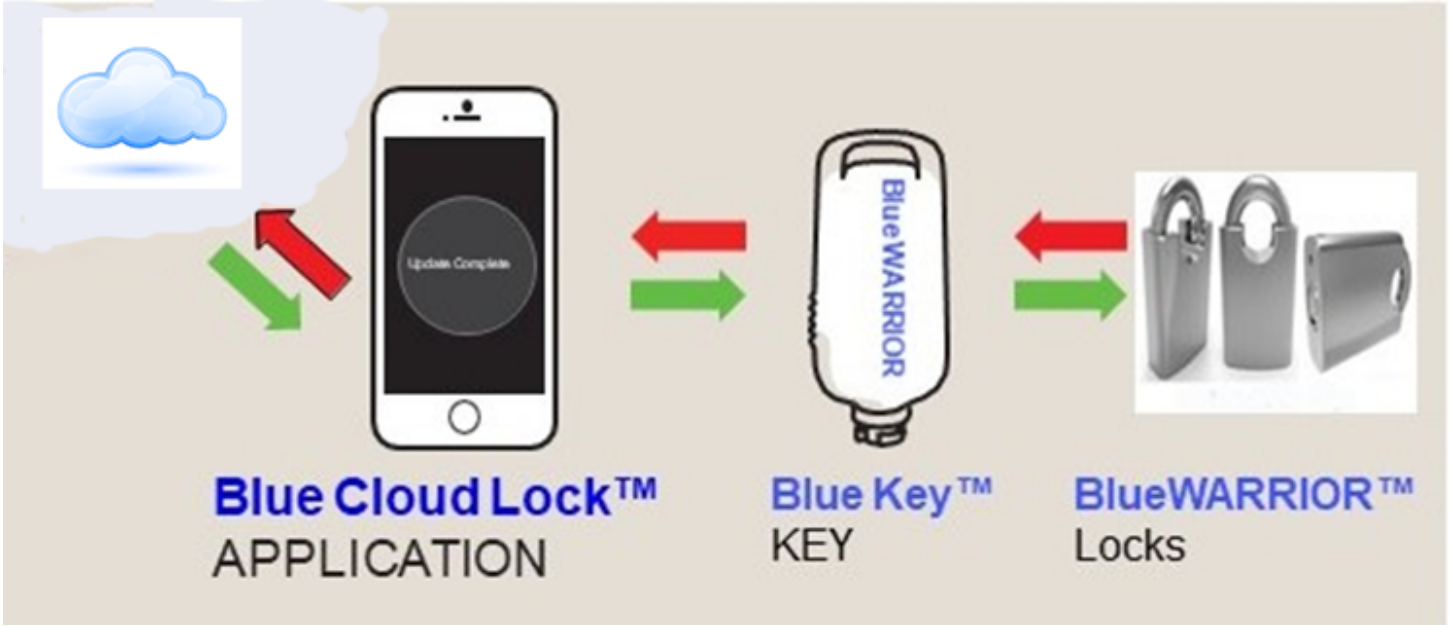
Generation & Distribution Assets require new tools to address the complex security scenarios facing critical infrastructure today. Secure, Encrypted Bluetooth locks are indispensable. The BlueWARRIOR Encrypted Bluetooth locks are used for internal use, locking devices on doors, machines, equipment cabinets, spares and switchgear equipment to prevent unauthorized access. In critical infrastructure environments, locks are often required to be temperature hardened (-40~+85C) and water-proof (IP65). BlueWARRIOR Encrypted Bluetooth Locks are certified for Indoor / Outdoor Use.

BlueKEY™ No wiring, No batteries & No Maintenance (Patent Pending)

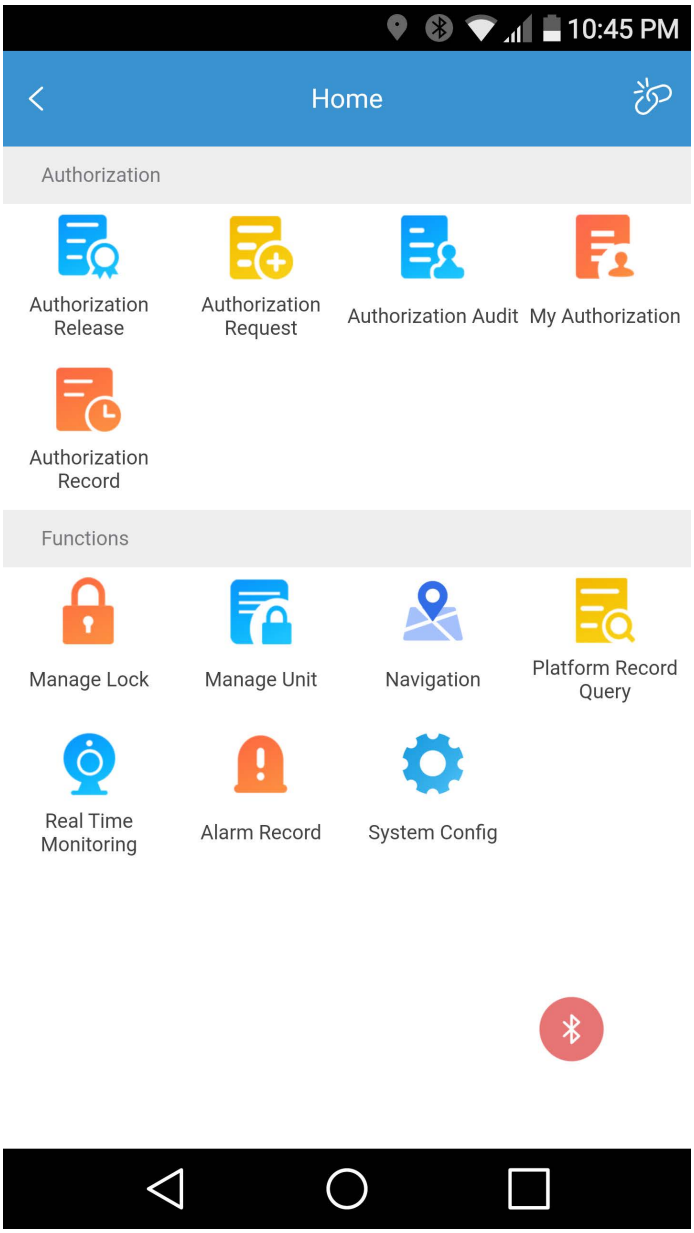
Critical infrastructure and Facilities

Operate across a wide range of geographic area and have the need for a large number of people needing to access multiple sites. Critical infrastructure companies often work with third-party contracting companies and/or who require temporary access to a remote site. Locking systems must accommodate these challenges, and provide a Full Audit Trail - of who, what, when and where. A complete log of each and every lock transaction. Time and date stamped! Critical infrastructure facilities can benefit from an encrypted security locking system that combines the best of electronic and mechanical security;

- Encrypted Bluetooth Keys are rechargeable
- Programmable Keys via the Worldwide Web
- Each Bluetooth Key has a unique Encrypted ID
- Each Bluetooth Lock has a unique Encrypted ID
- Encrypted Communication between Key & Lock
- No wiring required
- Full Audit Trail
- NIST Compliant
- Compliance for CIP Standards
- Made in USA
- IV Web & Data Security
- Low Cost



"Blue CloudLock" - Free Android Mobile Application for BlueWARRIOR Locks



-AUTHORIZATION SECTION -

Authorization Release- Administrative Assignment of Locks to keys & Users.

Authorization Request - Non-Administrative Staffer requesting Key Access to Locks.

Authorization Audit - Used to show which locks are authorized for a particular key.

My-Authorization - Not Used (Controllers)

Authorization Record - Locks that can be opened by the authorized key that corresponds to the credentials of the logged in user.

-Functions Section -

Manage Lock - Authorized locks that corresponds to the user's credentials.

Manage Unit - Manage locations of Smart Locks.

Navigation - Creating Locations that correspond to unit types.

Platform Record Query - Record Query for Blue Key and Smart-lock Authorizations.

Real-Time Monitoring - Lock Status

Alarm Record - (Future Development)
System Config - (Future Development)

Connect to BlueKey™

How to Achieve and Maintain US Physical Security and Regulatory Compliance

Today, NERC's Critical Infrastructure Protection (CIP) Standards require all electric utilities (public or private) to have a physical security plan and program in place to monitor and manage physical access to protect critical infrastructure, Cyber assets, and Bulk Electric System Cyber systems.

To comply with these standards, utilities must define operational or procedural controls to restrict physical access. For authorized individuals requiring physical access to critical infrastructure or physical security perimeters, utilities should - at a minimum:

• Implement a minimum of one physical access control system, although two or more control measures are recommended.

• Monitor unauthorized access through all physical access points.

• Maintain records (automated or manual) of entry — with time and date — for each individual with authorized access, unescorted access, or unauthorized access to physical access points.

• Issue an alarm or alert if unauthorized access is gained through physical access points.

• Keep physical access logs capturing date, time and location of individual's access.



Standard CIP-006 - Requires the initial identification and categorization of BES Cyber Systems and requires a minimum level of organizational, operational and procedural controls to mitigate risk to **BES Cyber Systems. (Bulk Electric System).** Established to manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES. (Audit Trail)

Standard CIP-014 - Established to identify and protect Transmission stations and Transmission Substations, Assets, and their associated primary Management Systems & Centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Utilities are Looking for: and Need

• Flexible, on the go - security access and key management for:
- Permanent Employees
- Contractors
- Part Time Employees
• Indoor and Outdoor locking and access points that support:
- Doors, machines, windows, shutters, cupboards, spares and cabinets
- Gates, Fencing, Switchgear Equipment
• Easy and Secure Web access to management software.
• Multiple administration capability Full Audit Trails, minimum administration time
• Easily support NERC CIP audits for physical security and forensic analysis
• Easy key and access management - individualized for different users and their requirements.
• Health and safety audit trails and records
• Integration possibilities with HR systems.

Low Cost BlueWARRIOR BlueKey™Locks are the Secure & Cost Effective Solution!



BlueWARRIOR Encrypted Bluetooth Padlocks for Power Generation & Distribution Facilities. A standard lock from the BlueKey™ Family.





Stainless Steel or Zinc Alloy. Can be customized for your company. (Address / Message / Logo). **No batteries, No wiring and No Maintenance**







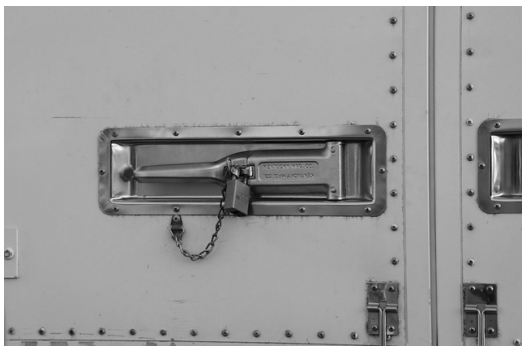
Indoor & Outdoor Rated
IP65
Hardened Shackles
NIST Compliant



BlueKey™ TRANSPORTATION SECURITY for the U.S.A.

Trailers, Containers, Storage Facilities

Global Reach for Security. Encrypted Bluetooth Keys and Padlocks provide a complete audit trail - recording ALL authorized opens and closes and UNAUTHORIZED attempts. Replaces seals which are easily cut and duplicated. REAL SECURITY!







The BlueWARRIOR Series 700

304 Stainless Steel Anti-Bolt Cutter - Encrypted - Very High Security

- **74 x 40 mm (2.9 x 1.57") Used For Trailers & Containers**
- **Key Is Separate**
- **Fully Encrypted**
- **Available in 304 Stainless Steel or ZINC Alloy**
- **Hardened-304 Stainless Steel Lock Housing Provides Rugged Resistance To Any Physical Attack**
- **Can Be Programmed Differently Or Alike (Multiple Keys or Multiple Locks)**
- **304 Stainless Steel Lock Body Provides Maximum Resistance Against Corrosion Indoors, Outdoors or in Marine Environments**
- **Drainage Holes Allow Moisture To Escape & Reduces Dirt Build Up**
- **Waterproof (IP67) Sealed Mechanism**
- **Encrypted Audit Trail - >60,000 Audit Events | >20,000 Cylinders**
- **Records both Authorized and Unauthorized Attempts to Unlock**
- **Complete Data Analytics**
- **Replaces SEALS with a lock that provides an Audit Trail**
- **Lower Cost than Key Systems**
- **Lock can be programmed to only open after delivery**
- **Eliminates Lock Picking & Duplicate Key Issues**

Cyber-Blue Cloud Database

- **Quality USA Made Product**
- **No Wires, No batteries, & No Maintenance**

If your padlock has keys - you have no security or audit trail

BlueWARRIOR Encrypted Bluetooth Traffic Enclosure Locks

No Wiring, No Batteries and No Maintenance

Meets & Exceeds Security requirements for NIST - Police, Fire, Traffic
Superior Encrypted Security
Manufactured to higher Standards & Tolerances

Exact Replacement Traffic Enclosure Lock

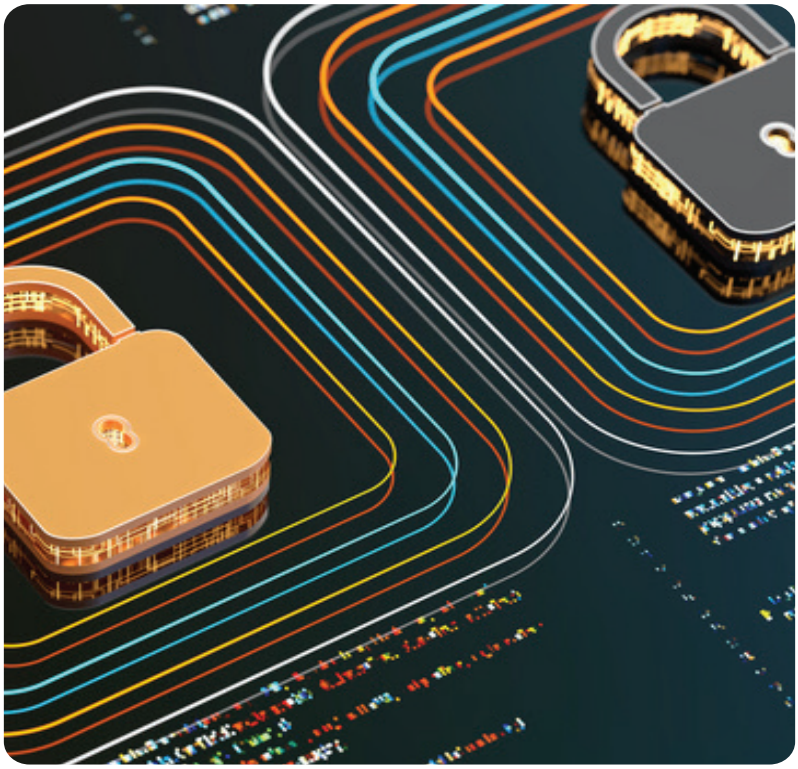
Exceeds NIST Security Standards
Easy Replacement
IV Web Hosting
Mobile Phone Updates & Authorization
Easy to use
Automatic Database



Email:
Sales@BlueWARRIOR.com
Sales@DYMEC.com

Websites: **www.BlueWARRIOR.com**
www.SecurityTransform.com
www.DYMEC.com





For more information visit www.BlueWARRIOR.com

© 2021 BlueWARRIOR All rights reserved.
BlueWARRIOR and other BlueWARRIOR product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of BlueWARRIOR All other trademarks referenced herein are the property of their respective owners.

BlueWARRIOR Bluetooth Locks Summary of Benefits

- When security and compliance are built-in from the outset, cloud lock systems are the most secure, less costly to maintain. BlueWARRIOR Bluetooth Locks deliver:

- Low Cost, Easy to Use (Automatic) - Exact Replacement Traffic Enclosure Lock & 304 Stainless Steel Padlocks
- **Provides a Full Audit Trail** of ALL - locking and unlocking transactions. Complete with date and time-stamp.
- Outdoor & Indoor Use Certified. Fully Temperature Hardened -40° ~ +85°C // Stainless Steel
- No Wiring or Batteries Required - All Power is provided by the Encrypted Bluetooth Key
- Every lock as its own unique encrypted ID
- Exact Physical Lock Replacement - no drilling, modification or changes needed. Less than 3 minutes to change a lock and add it to your inventory
- Supported on our Web Services - **"Cyber-Blue"** subscription
- Free Android Mobile phone Application - **"Blue-Cloudlock"** - automatically loads data transaction from the key to the database **"Cyber-Blue"** and updates permissions and authorizations from the database to the key.
- 5 Year Warranty on all Locks - 2 Year Warranty on Bluetooth Key
- Controls, Processes, and Automates Bluetooth Lock Security for continuous improvement
- Meets and Exceeds NIST Security Requirements for Critical Infrastructure Protection - includes Date and Time-stamp for every transaction. Includes recording of all unauthorized attempts to access locks.
- Asset-focused views to pinpoint specific types or groups of resources for compliance and security assessment and remediation activities
- Customizable benchmarks and policies to allow tailoring to suit site-specific compliance and security policies

BLUEWARRIOR



For more information visit www.BlueWARRIOR.com

© 2021 BlueWARRIOR - All rights reserved. (Patent Pending)
BlueWARRIOR, BlueKey and other BlueWARRIOR product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of BlueWARRIOR All other trademarks referenced herein are the property of their respective owners.