EntegraBLU™ Protection for Critical Medical Networks

Introduction:

A decade ago, hacking and other unauthorized entries into various networks were considered a nuisance generally carried out by individuals for either small monetary gain or simply for vandalism. In recent years, the threat has changed with the entry of sophisticated criminal gangs and nation states. Now such "hacking" can result in hundreds of millions of dollars of losses, from sabotage, extortion, and even terrorism. This growing threat has also captured the imagination of the media, which now reports on it extensively. What is clear is that the threat can no longer be ignored and the possible consequences now extend beyond insurable losses.

The fears of attacks against medical systems and institutions heightened in 2017 with the Petya cyber attacks. Hospitals within the United States and abroad were affected, including the Hollywood Presbyterian Hospital in Los Angeles which paid out $17,000 after hackers took control of its computers. Attacks like Petya are likely the tip of the iceberg. Future attacks are feared to target medical devices, records, and computers where a lack of remediation would result in potential severe injury or loss of life.

The threat to critical networks can no longer be ignored and solutions must be put into place as quickly as possible to protect them. Protecting these networks is now a fiduciary responsibility for all those involved.

EntegraBLU™:

While the scope of the problem and its dire consequences have only been recently recognized in the commercial world, America's intelligence community has been at the forefront of this issue for some time. Their requirements were to communicate securely, with minimal computational power, over any communications link (including multi-bounce satellites), and by transmitting through nearly any protocol. The EntegraBLU™ solution was born in this environment.

©2018 Entegra Technologies Inc. All Rights Reserved

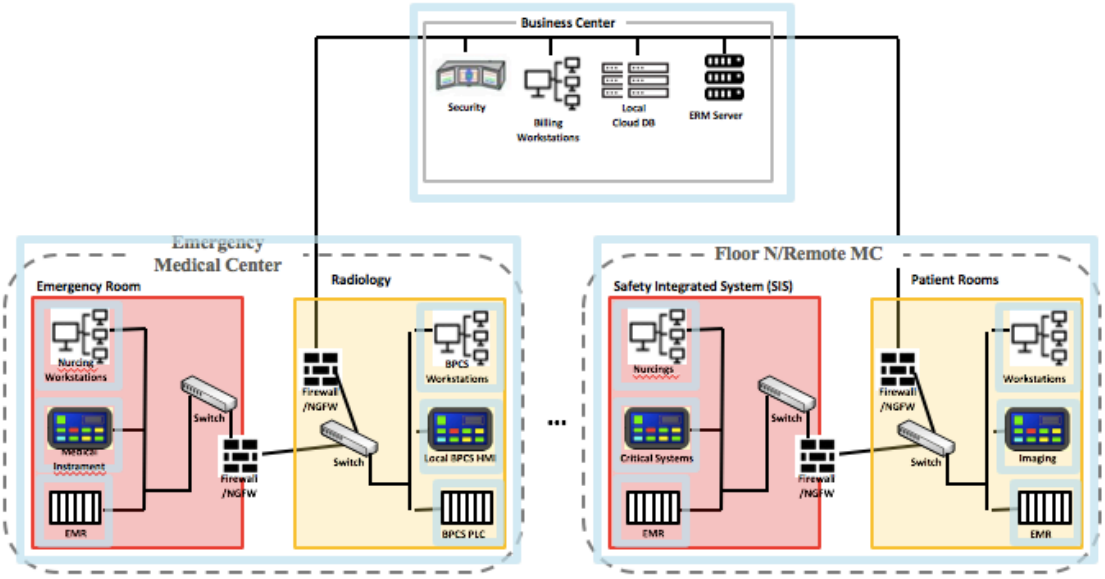
The solution has demonstrated its effectiveness, never having a known hack or breach or failing any certification or test attack in its 17 years of deployment. While it has evolved to function with the latest processors and operating systems, the basic algorithm has remained the same. This provides a proven solution and speaks to its known effectiveness.

To work seamlessly in any environment, the solution must provide a great deal of flexibility while maintaining simplicity and bulletproof encryption. EntegraBLU™ provides such a solution, using mutual-simultaneous key exchange to secure the communications link. The architecture of the solution allows this exchange to occur in an already encrypted environment, creating a stealthy system that is immune to man-in-the-middle attacks that can compromise conventional VPN's. Furthermore, the solution is agnostic to the data format or means of communication. Data is wrapped in a protective encrypted shroud and transported across the communications link as if by Ethernet, and then unwrapped on the other side and sent on its way. To the entities on either side, individual or LAN, it is as if the two are connected by Ethernet.

The important aspect with the system is that a data and protocol agnostic transmission link is formed that is unbreakably secured between the edge device and its ecosystem and the EntegraBLU™ Server and its ecosystem. The two will appear to be linked by Ethernet, but the data is otherwise unaffected. This means that legacy systems or newly deployed systems can function without even knowing that the security solution is active.

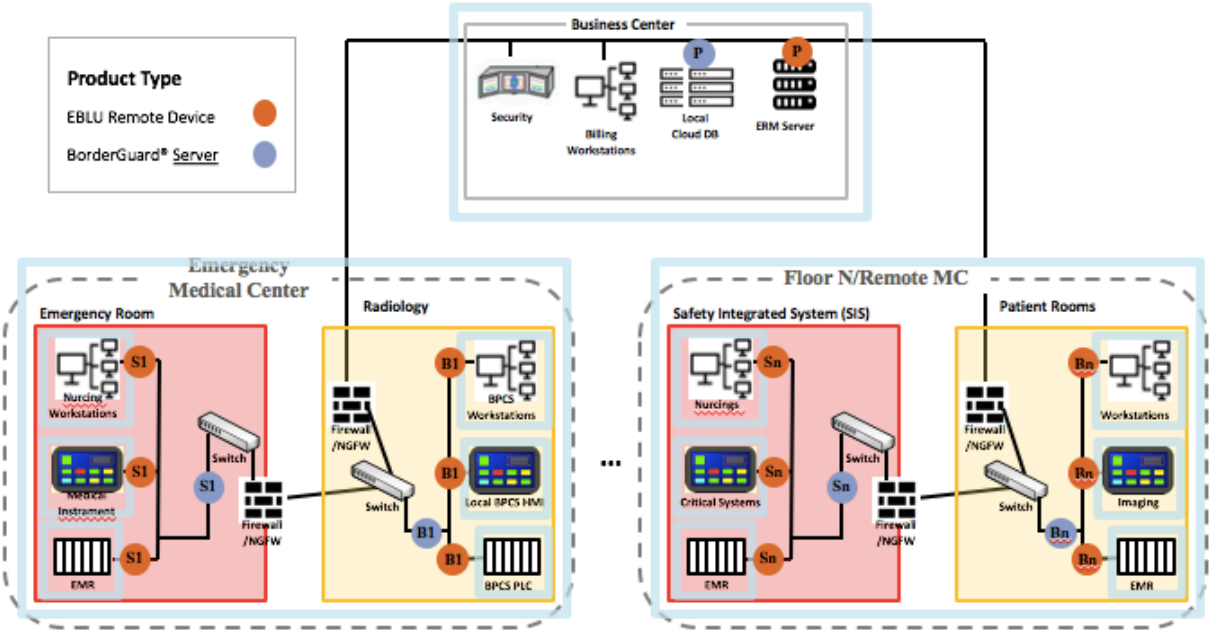
Any collection of edge devices and EntegraBLU™ Server can be supported, allowing the customer to establish the isolation and security relationships of their choice.

In a general medical center structure, one would usually see architectures similar to that shown below:



©2018 Entegra Technologies Inc. All Rights Reserved

With EntegraBLU™, the architecture is segregated and isolated so that only predetermined contact is allowed, as shown below:



The EntegraBLU™ edge devices working with the EntegraBLU™ Server provide the security the network needs without affecting the operations of the devices within the network, or any of the other security efforts (such as a firewall) that might be in place. This provides the defense-in-depth of the concept.

How would this solution apply to a real-world case?

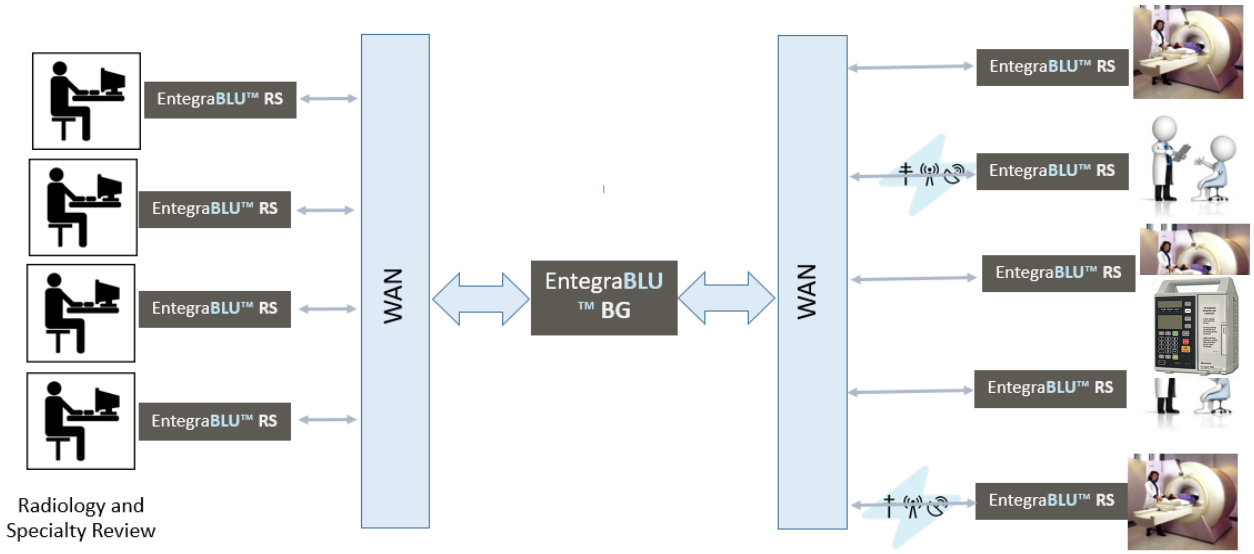
EntegraBLU™ Medical Data:

Take a real-world case, simplified for this discussion. At a wide variety of locations there are a number of edge devices, in this case imagine that these are medical devices (such as MRIs, diagnostic cameras, or infusion pumps). In many cases, the data from these device needs to be transferred either to a specialist or remote diagnostic computer that processes the data. The results of these reviews, or processed data, must then be transferred back to the attending physician. All of these data transfers must be secured to comply with HIPAA regulations and general patient privacy concerns. There is great economic value in being able to leverage existing Wide Area Networks to connect each of the nodes of this data transaction. This means that the wide variety of available networks and cloud-based services would be very valuable to use if one can guarantee security. It is essential that this data not be compromised, yet it would be exposed over any number of different networks.

©2018 Entegra Technologies Inc. All Rights Reserved

EntegraBLU™ provides this security by placing a small (iPhone-sized) edge device at each node of the network, or an embedded solution within the medical device itself. This data is encrypted and transmitted to the EntegraBLU™ Server, which sends it to only acceptable locations, for example, the data center, radiologist, or another specialist. Similarly, information from the data center or various specialists can be transmitted safely via the EntegraBLU™ Server to the attending physician. All of this is done securely and transparently. In the first typical example, we have a collection of MRIs which generate significant data, all of which will need to be reviewed by a radiologist or another specialist, with the results forwarded back to the attending physician.

All of the nodes in this network can be separated by large, even global distances and the data can be in transit over numerous networks:

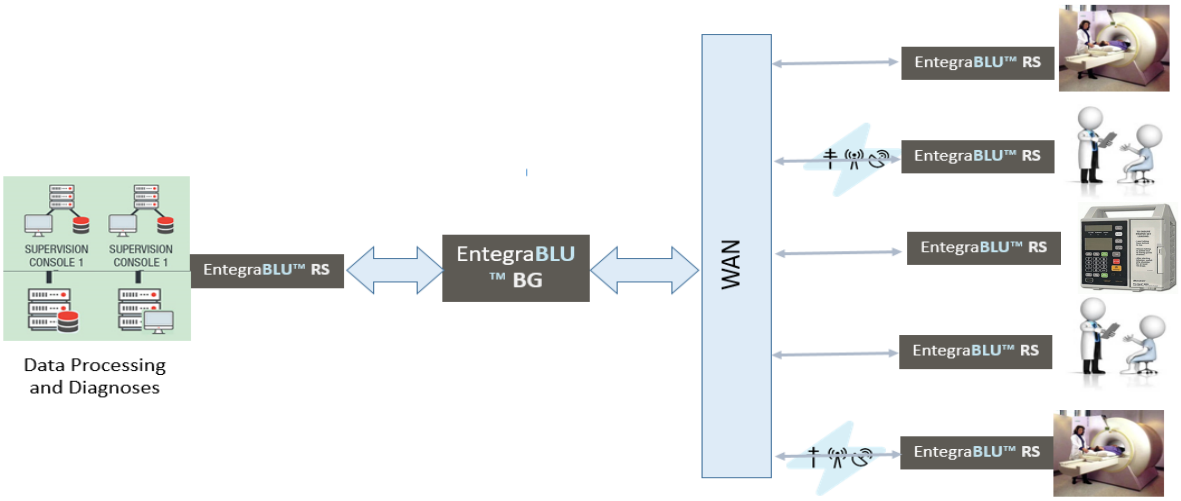


The EntegraBLU™ solution allows these communications to proceed transparently over untrusted networks while remaining unseen by hackers. Patient privacy is protected and legal requirements are satisfied.

Consider a second example from the medical world. In this case, EntegraBLU™ is protecting patient data while allowing large-scale data processing, image enhancements, and recognition in what will likely be one of the largest innovations in future medical care: computer-assisted diagnosis and treatment. In this case, the data is also first generated in a medical device. While an MRI is shown in the graphic, the device could just as easily be a smaller device with an embedded EntegraBLU™ solution. In this case, imagine, for example, a small camera with EntegraBLU™ embedded in the camera chip set. The images taken by this camera will then be used for diagnostic support. For example, an image of several wavelengths of a skin anomaly could be sent to computers for image processing and the resulting images subjected to automated review from a database. The processed information could them be sent back to the

©2018 Entegra Technologies Inc. All Rights Reserved

attending physician along with any other data indicated by the review. Schematically, this is shown below:



Of course, any number of additional nodes or other features could be incorporated to tailor the network to the user's requirements.

Regardless of the complexity of the network, the EntegraBLU™ solution will function in a conceptually similar fashion. Data will be protected with effectively unbreakable cryptographic techniques, all while remaining transparent to the user.

Conclusion:

Critical networks require protection and EntegraBLU™ is the solution that stops the attack on Day 0. EntegraBLU™ security solutions wrap the critical network systems into secure enclaves which are invisible to the outside world. Within the enclave the network is completely flexible in architecture and is suitable for the protection of legacy systems. Encrypted communication can only occur between EntegraBLU™ components by a L2 layer encrypted link after the simultaneous exchange of the SE-IKE key set. The solution is intrinsically stealthy and is easy to deploy and maintain. With EntegraBLU™ the economic benefits of connectivity can be fully realized in critical networks while the operators can be confident of protection from cyber-attacks.

To learn more about security for data transit, contact us:

EntegraBLU™

800-766-2026

©2018 Entegra Technologies Inc. All Rights Reserved