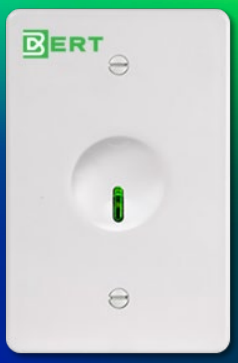

Security Features

BERT's robust slate of security features helps keep your networks protected and your data secure.

Enterprise-Level Encryption

BERT devices employ state-of-the-art end-to-end encryption, ensuring the highest standards of Wi-Fi security and data integrity. This Enterprise-level encryption, combined with strong password support, provides a formidable defense against unauthorized access.

Advanced Endpoint Protection

BERT devices are designed with a security-first approach, significantly minimizing the attack surface through several key features:

- **Limited UDP Port Usage**
  Devices are configured to communicate solely through two UDP (User Datagram Protocol) ports, enhancing security by restricting potential entry points.
- **UDP Benefits**
  User Datagram Protocol is lightweight compared to TCP (Transmission Control Protocol), enabling faster data transmission. This means less resource consumption, which is ideal for IoT applications.
- **Exclusion of TCP Support**
  By not supporting TCP, BERT devices eliminate a protocol susceptible to exploitation, further bolstering security.

On-Premises Software

Our software operates solely on your local equipment, eliminating the need for external communication and insulation from internet-based threats.

Recommended Network Isolation Strategies

To enhance the security of your BERT devices and overall IoT network, consider implementing additional isolation measures.

Internal Network Isolation

Adopt a segmented network strategy to create distinct boundaries between operational and IoT networks:

- Create a separate network (e.g., unique Wi-Fi SSID and password) for IoT devices.
- Segmentation excludes IoT devices from accessing your main network and allows granular management of IoT activity, including MAC address authentication. We are pleased to provide a list of devices ahead of installation.

BERTBRAIN.COM
489 Devon Park Drive, Suite 302
Wayne, Pennsylvania 19087

484.690.3820
sales@bertbrain.com

03/19/25