

**SECURE**  
your infrastructure

**PROTECT**  
your investment

**PREVENT**  
unauthorized access

## Biometric Access Control

M610 / R610 Access Control System

- Configuration – Dual Units. One at access location and one inside secure area
- Communication – All communication is encrypted
- Certification – GSA approved and catalogued, ongoing FIPS 201 compliance



## Security

- Enhanced biometric security
  - o No fingerprint images stored
  - o Impossible to reverse engineer fingerprint
- Encrypted biometric templates
- Biometric access to software
- No direct communication from control unit to door
- All units operate independently of network
- 8 hour battery backup
- Dual units for each access point
- Base unit located on inside of protected area
- Anti-tamper systems in unit and door
- Forced door/propped door notification
- Live finger detection

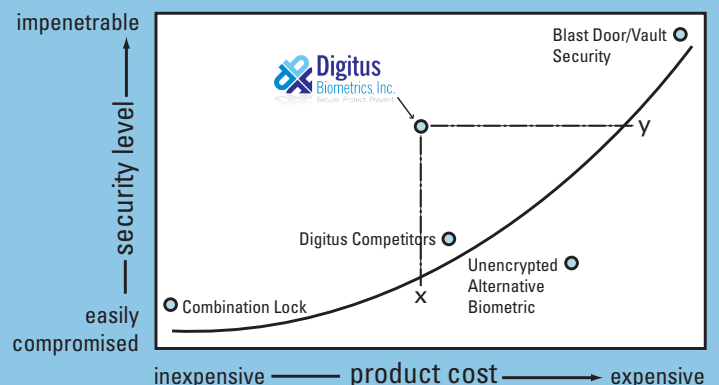
## Implementation & Operation

- Easily installed and configured
- Easily networked
- Easy and fast enrollment
- Cost effective and customizable
- Ensures privacy and 4th Amendment protection
- **Networked operation (TCP/IP)**
  - o All system and software management via PC
  - o Centralized enrollment
  - o Remotely lock/unlock secure doors
- **Standalone operation**
  - o Enrollment performed at the unit
  - o Biometrically protected menus
  - o Operates independently of software and PC
- **Integrated operation**
  - o Scalable to existing enterprise and access control systems

## Why Digitus?

**Simply Secure** – The Digitus solution is significantly more secure and cost effective than competitive systems and traditional access protocols.

x—the Digitus Access System cost  
y—the Digitus Access System security level



For more information, please contact Digitus directly, or visit [www.digitus-biometrics.com](http://www.digitus-biometrics.com)