DMP Network Security is Serious Business

Synopsis: Considering all the reports of hacks and breaches, you might get the feeling that data protection measures are not all they should be. More than ever before the product you select to protect your home and business is of utmost importance. The increasing availability of mobile access to home and commercial security systems via apps has escalated concerns. But based on the technology used in DMP systems and their record for maintaining solid data security, it is clear there is someone you can trust.

Considering all the reports of hacks and breaches, you might get the feeling that data protection measures are not all they should be. More than ever before the product you select to protect your home and business is of utmost importance. The increasing availability of mobile access to home and commercial security systems via apps has escalated concerns. But based on the technology used in DMP systems and their record for maintaining solid data security, it is clear there is someone you can trust. DMP's proven history in the high-security space began in the early 1990s with the first use of data networks for alarm panel communication, including the internet. That led to their first-ever UL High-Line Security Listings for that application.

A DMP technology developed for these high-security applications is called AdaptiveTechnology™. This exclusive DMP feature seamlessly switches between communication links – cellular and network – with no lost supervision polling, while maintaining panel substitution detection. 128-bit AES, and subsequently 256-bit AES encryption, earned DMP the first NIST certification for encrypted intrusion panels. The focus on system security continued in the early 2000s when DMP added wireless technology. This commercial-grade, two-way wireless technology incorporated frequency-hopping and spread-spectrum technology. It randomly changes channels every 32 milliseconds, just like many military-specified wireless radios. That innovation enabled DMP to earn UL Commercial Fire Listings for their premise's wireless system. DMP wireless technology is rock solid, and, with a range of over 1.5 miles, it sets the standard that others are measured by.

When DMP added cellular communication to their control panels several years ago, they determined the most secure solution was to transmit alarm signals directly from the control panel to the central station receiver with no retransmission or relaying of signals. All alarm communication goes directly to the central station receivers, where substitution detection and patented reverse-polling methodologies are maintained. The increasing availability of smartphones and mobile devices opened the door to amazing new mobile technologies and management capabilities for alarm systems. As DMP developed apps and browser interfaces, they took the most conservative approach. They adhered to Internet security industry standards and designed both the architecture and logic of solutions to incorporate security at every step. "We take the security of our equipment and our apps and software very seriously," says Jeff Britton, VP of Product Design. "From the architecture of the hardware to the implementation of the software and maintenance of our servers, security is at the forefront. You can count on that."

The list of features in place to ensure the security of DMP cloud-based solutions is long:

- 10-character app and browser passwords, with complex combination of non-alpha characters required
- Three invalid codes entered will log users out
- Video stream IDs change frequently, with URLs randomly generated at time of viewing
- All video streams over closed and encrypted VPN, and requires authentication at the camera
- Panel user-code, email address, and password authentication required for login
- Touch ID supported as an option to launch the app
- Account enumeration prohibited
- 2048-bit RSA and 256-bit AES used for encryption
- No user feedback provided to users regarding email address validity
- DMP hardware and software is readily updatable
- Third-party scheduled penetration testing
- Active monitoring and patching of all discovered vulnerabilities and malware

Additionally, retailers who use Credit Card Processing Services must follow The Payment Industry Security Standard compliance rules for their network and internet connectivity. When a DMP system is deployed in such an environment, we take care that our cameras and our EasyConnect™ network communication meet those requirements so that retailers can use their internet infrastructure at the lowest cost to them. DMP works to ensure that retailers have the practicality of a safe and secure building, stock room, and showroom, as well as a safe data connection.

Digital security should not be taken lightly or ignored. Hackers are intent on breaking into systems, whether to collect data, incur online vandalism or worse. Whether protecting home and family, retail establishments, professional spaces, bank chains or government facilities, DMP technology provides some of the most secure solutions available.